SPEC Kit 360

Learning Analytics

September 2018

ASSOCIATION OF RESEARCH LIBRARIES

SPEC Kit 360

Learning Analytics

September 2018

Michael R. Perry, Northwestern University
Kristin A. Briney, University of Wisconsin-Milwaukee
Abigail Goben, University of Illinois at Chicago
Andrew Asher, Indiana University Bloomington
Kyle M. L. Jones, Indiana University-Indianapolis (IUPUI)
M. Brooke Robertshaw, Oregon State University
Dorothea Salo, University of Wisconsin-Madison

ASSOCIATION OF RESEARCH LIBRARIES



SPEC Series Editor: Lee Anne George

Association of Research Libraries
21 Dupont Circle, NW
Suite 800
Washington, DC 20036-1118
T 202.296.2296
F 202.872.0884

ARL.org
pubs@arl.org

ISBN 978-1-59407-998-6 print
ISBN 978-1-59407-999-3 online

Copyright © 2018

This compilation is copyrighted by the Association of Research Libraries. ARL grants blanket permission to reproduce and distribute copies of this work for nonprofit, educational, or library purposes, provided that copies are distributed at or below cost and that ARL, the source, and copyright notice are included on each copy. This permission is in addition to rights of reproduction granted under Sections 107, 108, and other provisions of the US Copyright Act.

NOTE: The executive summary (pages 2–6) is licensed under a Creative Commons Attribution 4.0 International License.

Table of Contents

Survey Results

Executive Summary 2
Survey Questions and Responses 7
Responding Institutions 41

Representative Documents

Library Privacy Statements and Policies
University of California, Irvine Libraries
UC Irvine Libraries Privacy Statement 44
Duke University Libraries
Privacy 45
Emory University Libraries
Policy on the Collection, Use, and Disclosure of Personal Information 48
University of Florida Libraries
Privacy Policy 52
Georgetown University Library
Statement on Data Use for Library Assessment Purposes 54
Indiana University Bloomington Libraries
Privacy Policy 55
University of Maryland Libraries
Privacy Information 60
Pennsylvania State University Libraries
Policy UL-AD08 Confidentiality and Privacy of Patron Library Records 62
Syracuse University Libraries
Privacy Policy 65
Temple University Libraries
Ask a Librarian: Privacy Policy 72
Washington University in St. Louis Libraries
WU Libraries Privacy Statement 73

Institution Privacy Policies
Colorado State University
Information Collection and Personal Records Privacy 78
Indiana University Bloomington
Privacy of Electronic Information and Information Technology Resources ..82
Pennsylvania State University
AD53 Privacy Policy 88
University of Virginia
IRM-012: Privacy and Confidentiality of University Information 94
Western University
Official Student Record Information Privacy Policy 100

Data Security Policies
Boston College
Data Security Policy 107
University of Florida
Information Security 115
Johns Hopkins University
Policy on Access and Retention of Research Data and Materials 117
Homewood Institutional Review Board | Data Security 122
Louisiana State University
Security of Data 124
University of Massachusetts Amherst
Information Security Policy - Draft 128
University of Minnesota
Sharing Data with University Educational and Administrative Audiences ... 134
University of Virginia
Information Security at UVA | Data Protection 136
University of Waterloo
Guidelines for Managing Student Information for Faculties, Academic Departments and Schools 140

Selected Resources

Books, Reports, Journal Articles, and Government Information 146
Consortia 147
Data Handling Policies 147
Privacy Statements and Policies 149
Institutional Data Requests 151
Training 151

This page intentionally left blank

Survey Results

Executive Summary

Introduction

In recent years, a line of research has appeared in the library literature under the auspices of "Library Value" or "Library Impact" studies. The purpose of this research is to determine how library usage (e.g., of resources, services, spaces, etc.), relates to student learning and academic achievement outcomes. As a result of this, academic libraries are increasingly building capacity for, and participating in learning analytics (LA), which is defined as the "measurement, collection, analysis, and reporting of [student and other data] for the purposes of understanding and optimizing learning and the environments in which it occurs" (LAK, 2011). Using LA, libraries and their institutions believe they are more prepared to describe (what is happening?), diagnose (why did it happen?), and predict (what is likely to happen?) factors that influence or inhibit student learning, and prescribe (what should we do about it?) interventions. The success of LA depends in part on an institution's ability to connect campus information systems—including those under the purview of libraries—to aggregate and analyze data about student. But as institutions continue to surface granular data and information about student life, the risk to student privacy grows. It is unclear how libraries are addressing those risks.

The purpose of this survey was to illuminate current practices, policies, and ethical issues around libraries and learning analytics. This environmental scan explores how ARL member institutions are navigating the balance between gathering and managing data in support of learning analytics initiatives and attending to the profession's ethics commitments. To these ends, the survey questions sought to answer these broad questions: how are academic libraries planning for, adopting, and participating in learning analytics initiatives?; what mechanisms do they use to maintain data security and privacy?; what ethical issues do they encounter when participating in learning analytics?; and how do they negotiate and resolve those issues?

The survey was conducted between April 30 and June 15, 2018. Fifty-three of the 125 ARL libraries responded to the survey for a 42% response rate.

Learning Analytics Initiative Participation (Q1—Q6)

The introductory questions asked about current participation in learning analytics initiatives within the libraries, focusing on participation, storage, and types of data collected both with or without personal identifiers.

Of the 53 responding libraries, 83% indicated that they were participating in learning analytics projects, suggesting broad uptake across ARL institutions. Further, nearly three-quarters of respondents indicated that they had staff allocated to these types of projects. This high percentage of uptake and the

dedication of staff to positions supporting learning analytics initiatives suggests the expansion of this type of metric as well as administrative perception of the importance of these efforts.

Responses about institutional data storage for learning analytics data revealed a variety of storage strategies. Respondents had the option to select multiple answers. The most common LA data storage location is a central data warehouse (41 responses, or 80%). Almost as many respondents (38 or 75%) reported that data is stored by the unit that collects it. Nearly 20% of respondents indicated that they store data in a distinct learning analytics warehouse and 20% also indicated that another repository was being used.

Respondents were asked to identify what types of library data are collected and whether this data is collected with or without individual patron identifiers. The most commonly reported types of data captured concern patron interaction with library staff (research consultations, reference, instruction) and materials usage (print and electronic). These data points are being gathered by more than 80% of respondents.

The majority of respondents indicated that individuals (via unique identifiers) are not tracked. The two highest measures tracked with personal identifiers are tied to collections: physical circulation and interlibrary loan information. While students are unlikely to be directly identified for coursework and workshop attendance, individual information is required for delivery of materials.

Library Practices (Q7—Q12)

Questions about library practices covered who participates in collecting and analyzing information and data retention durations.

All of the respondents reported that staff librarians gather library LA data, which corresponds with the regular collection of reference and instruction data. There was also nearly universal agreement that librarians are engaged with analyzing the data (43 responses, or 96%). Non-librarian staff also frequently gather LA data (40 or 89%), though fewer are engaged in analyzing the data (29 or 64%).

Fewer than half of the responding institutions reported having a records-management schedule or policy that controls the retention of learning analytics data. The survey results did not show a difference between public or private institutions regarding the existence of a retention policy. Only two institutions indicated that their policies had changed because of learning analytics. Text responses about the duration for library learning analytics data retention reveals that institutions that do not have a retention schedule are more likely to keep data indefinitely. At institutions that have a policy, retention periods vary by data type and collection purpose, with periods between one month (electronic vendor data) to ten years (circulation) data being reported.

Library and Institutional Data Sharing (Q13—Q24)

Fewer than half of respondents reported sharing data with other departments on campus or to a central warehouse, although twenty percent did indicate that they were planning to begin doing so within the next 6–12 months.

Interestingly, the data most often shared with other departments concerns collections usage—circulation and e-resource usage—rather than data about patron interaction with library staff. This may be tied to the need to provide contextual numbers to obtain more funding for materials budgets; whether this is directly related to department or university level learning analytics is unclear.

The respondents who indicated that they are not sharing data beyond the library cited privacy and confidentiality as the primary concerns, although lack of resources was also ranked highly. Other reasons included that the library is not seen as a data source and that there are a lack of campus initiatives or requests for the data.

Only eight of the respondents indicated they place restrictions on how shared data is used by other departments; while institutional data shared with the library comes with greater acknowledged restrictions.

Several questions focused on the perceived importance of library LA. The majority of respondents indicated that, in response to institutional LA efforts, they are collecting the same or more data with personal identifiers than they had previously. However, despite this increase, only about half felt that library data was important to campus-level initiatives. This is markedly smaller than the 80% of respondents who felt that library participation in LA was important to library administration, suggesting a greater value is being placed internally than externally on these initiatives.

Data Protections (Q25—Q28)

This section of the survey specifically dealt with library policies, practices, and training around data protections (e.g., handling and management).

The most common data protections identified in learning analytics projects include limiting staff access to unanalyzed data, removing direct identifiers, limiting the scope of data collection, and securing storage. Few libraries reported securing data during transit, deleting data, or limiting retention. Coupled with previous results indicating long data retention periods, this suggests that libraries do not consider data deletion or limited retention as a necessary data protection strategy.

Only 16 respondents answered a question about library anonymization techniques; of those, several described relying on the office of institutional research to de-identify the data. Others described basic de-identification such as removing student ID numbers and names and masking identifiers, though these practices are not equivalent to full anonymization.

Only two libraries have a learning analytics data management plan. A few libraries indicated that they intend to make a data management plan. When asked for plan details, several libraries linked to a webpage on data management plans for researchers with little indication as to whether these practices were used internally on library data.

Privacy Policies and Practices (Q29—Q36)

A particular focus for this survey is the privacy policies relevant to library learning analytics and how they are implemented by the library.

While 45 respondents (90%) indicated that their institution has a privacy policy, only 31 of those have a separate library privacy policy. Most of those library policies link to the university policy, state laws on library records, and to the ALA Code of Ethics. Fewer than half point to software terms of service, the 2001 USA PATRIOT Act, the 1974 Family Educational Rights and Privacy Act (FERPA), or another document.

There is a general lack of consistency regarding policy review and revision. Several respondents indicated updates happen “as needed” or “periodically” without further detail. Notably, a couple mentioned that they are currently reviewing these policies for update in 2018, with at least one mention of making changes based on the European Union’s General Data Protection Regulation (GDPR) requirements. Others are reviewed every few years, one is updated when laws change, and one was last updated nearly 15 years ago. Most respondents indicated that LA has not caused changes in their privacy policies. Only one respondent indicated that they created a “Responsible Use of Library Data” statement in alignment with their learning analytics project.

Eighteen libraries (42%) inform students about library learning analytics initiatives. However, 11 of these—nearly three-quarters—indicated that there was no mechanism for students to opt out or that any kind of non-participation option was available.

The majority of respondents (28 or 70%) obtain Institutional Review Board approval for learning analytics projects. Those who indicated that they did not seek approval commented that the projects were for non-research purposes, library internal use, or process improvements, all of which are typically exempt from IRB oversight. Two institutions indicated that when they used data beyond strictly internal process review, they obtained consent from students and allowed participants to opt out.

Sixty percent of respondents indicated that they review FERPA with staff members for their learning analytics work. Several comments indicate a reliance on general institutional training, without further specific training regarding LA.

Procedures (Q37—Q40)

In addition to understanding the overarching policies about data handling and privacy, the survey sought to understand the day-to-day documentation and training available to prepare librarians gathering data and participating in LA initiatives to meet best practices or respond to data requests.

Internal staff guidelines and documentation are only available at one-quarter of 44 responding institutions. These include both internal and external training, planning documents, and a document specifying levels of data access (unanalyzed data, de-identified, etc.) One interesting response indicated that not only did they provide information about how patron data was used, they also had a statement that addressed the data gathered about the librarians as well.

Only a third of 45 responding libraries have a process for handling external requests from subject departments or other campus entities for library data. Comments indicate that administrators or staff responsible for assessment may be called upon to review these requests on an ad hoc basis. One respondent reported that "we would cooperate and collaborate with any department requesting institutional data" without further suggesting any restrictions or parameters under which the data might be shared.

Library staff who are involved in learning analytics projects are most likely to receive training on specific tools and IRB and FERPA requirements. Some of the responding libraries also provide training on data visualization, security, and handling (e.g., cleaning). Seven respondents (16%) indicated that librarians received no training for learning analytics projects.

Partnerships (Q41—Q43)

The survey next asked whether the library is participating in any learning analytics partnerships either on or beyond campus. Almost 40% of respondents indicated they participate in LA initiatives alongside campus units such as the Office of Institutional Research, the Writing Center, Information Technology, Provost, Office of Assessment, and Undergraduate Affairs. A third of the respondents are working with consortia, such as the Greater Western Library Alliance Student Success Initiative and Unizin.

A final question offered respondents the opportunity to add anything the survey missed. A majority of respondents pointed out that learning analytics projects at their institutions and their libraries are nascent. They generally indicated an interest and willingness to engage in the gathering and assessment of this data without reservations. Only one institution clearly stated that they were not undertaking learning analytics projects and did not intend to do so.

Recommendations

Overall, the survey results suggest that participation in library learning analytics, broadly defined, is of great interest to ARL libraries, with the majority of respondents participating in some sort of initiative within their library, if not yet within their institution. Libraries are increasingly capturing learning analytics data with personal identifiers, although little data is being formally or regularly shared with

campus partners or externally to consortia; however, the comments suggest an interest in engaging with both. Currently, libraries are inconsistent in whether they have a distinct data policy, staff documentation on data handling, and comprehensive internal training. This informs the recommendations set out below:

- Libraries should put in place a schedule for reviewing and/or developing privacy and data management policies. This process should be handled by an informed and dedicated committee, office, or individual. Policies should be written in clear, concise, and understandable language. Wherever possible, actual systems or data types should be identified. Policies should include a revision history, approval process, and last reviewed date, as well as contact information for questions. Policies should link, as appropriate, to other governing documents, such as university policies, state and federal laws, and the ALA Code of Ethics.
- Libraries should expand training on data handling best practices that goes beyond institutional FERPA and IRB training. Library staff would most benefit from training on underutilized data protection practices identified in the survey results, including: technical protections, like encryption, for both storage and transit; processes for data minimization, including limiting data collection and retention times; and anonymization strategies. Libraries commit to protecting the privacy of the information about their users and their information habits; such commitments should also be applied to user data they keep and share.
- As many projects are perceived to be for internal use only, the Institutional Review Board may not be contacted, even when the data are subsequently used for research. Similarly, many IRBs do not see data already collected as carrying potential for harm. Libraries should develop best practices for assessing the ethical and personal privacy risk to students internally, rather than relying on IRBs, regardless of whether they have immediate plans to disseminate findings from their work.
- Libraries should be more transparent about their student learning analytics projects. Only one respondent provided a document outlining learning analytics projects, and it is unclear whether the document was ever publicly available. This transparency includes engaging with students to inform them about what data is collected about them and how it is used.

Survey Questions and Responses

The SPEC Survey on Learning Analytics was designed by **Andrew Asher**, Assessment Librarian at the Indiana University Bloomington Libraries; **Kristin A. Briney**, Data Services Librarian at the University of Wisconsin-Milwaukee; **Abigail Goben**, Associate Professor, Information Services and Liaison Librarian at the University of Illinois at Chicago; **Kyle M. L. Jones**, Assistant Professor, Department of Library and Information Science at Indiana University-Indianapolis; **Michael R. Perry**, Head of Assessment & Planning at Northwestern University Library; **M. Brooke Robertshaw**, Assistant Professor & Assessment Librarian at Oregon State University Libraries & Press; and **Dorothea Salo**, Faculty Associate in the Information School at the University of Wisconsin-Madison. These results are based on responses from 53 of the 125 ARL member libraries (42%) by the deadline of June 15, 2018. The survey's introductory text and questions are reproduced below, followed by the response data and selected comments from the respondents.

Learning analytics is commonly defined as the "measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs" (Siemens, 2012). In recent years, library researchers have begun pursuing a research agenda under the auspices of "Library Value" to determine how library usage (e.g., resources, services, spaces, etc.) as expressed in student data is related with and improves student learning outcomes. Effectively, Library Value research is aligned with learning analytics goals.

The purpose of this survey is to illuminate current practices, policies, and ethical issues around libraries and learning analytics. This environmental scan will explore how ARL member institutions are navigating the balance between gathering and managing data in support of learning analytics initiatives and attending to the profession's ethics commitments. To these ends, the survey will seek to answer these broad questions: how are academic libraries planning for, adopting, and participating in learning analytics initiatives?; what mechanisms do they use to maintain data security and privacy?; what ethical issues do they encounter when participating in learning analytics?; and how do they negotiate and resolve those issues?

LEARNING ANALYTICS ENGAGEMENT

Learning analytics is commonly defined as the "measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs" (Siemens, 2012).

Learning analytics include library assessment projects that utilize educational and institutional data, data analysis methods, and share similar goals of other non-library learning analytics work. Please

consider your library assessment work as being situated under this inclusive term when answering the survey questions.

1. **Is your institution engaged in learning analytics projects/initiatives as defined above?** N=53

Yes	43	81%
No	10	19%

Comments N=19

Answered Yes N=15

Based on my initiatives only. They do not do any of this relating to the library unless we initiate the project.

But only in ad hoc projects.

Here it is referred to as Learning Outcomes, although there is no formal office on campus doing this that we are aware of.

In a very rudimentary way, the university is engaged in learning analytics. I believe this is done mostly for reporting purposes at a very high level. I am not aware of college or department level analytics projects, except for those happening in my own Research and Instruction Services department.

In the context of university-wide assessment and accreditation, the university conducts an evaluation of student portfolios as well as writing samples. These are qualitative assessments, not quantitative.

Isolated discussions on the learning environment but nothing formal. Some indicators are reported for strategic theme of outstanding academic programming.

Mostly the User Experience (UX) Department, the READ scale through the Research Instruction and Outreach (RIO) Department.

One-off projects to study things like impact of learning commons, embedded librarianship.

The Assessment & User Experience (AUX) Department, in collaboration with other departments, engages in learning analytics projects and initiatives. In the Libraries, assessment and analytics-based work is often tied to either library strategic initiatives and goals, or departments goals. We define assessment as a set of activities that allow us to understand our impact upon institutional outcomes, identify user needs and satisfaction, and can be used to improve collections and library services. Other departments within the library pursue their own analysis of data. These efforts are often very contextual designed to seek feedback for service or instruction improvement. One of the most robust examples includes a yearlong multi-modal learning assessment from the doctoral program in the School of Education. Students are assessed various ways, such as after online synchronous workshops; emails; research consultations, and after face-to-face orientations. Individual librarians also collect learning statistics through their instruction and outreach. Our library also administratively houses a department responsible for robust professional development for teaching faculty—and there is a great deal of assessment and analysis around the work such as exploration of short-term, mid-term, and long-term learning outcomes associated with the activities of this particular department. Their assessment and analytics are directed to the provost of the university and not included in library service design, assessment, or collection assessment so for the purposes of this survey, this unit has not been included because most other programs like this at other institutions are housed administratively outside of the library.

The terms “data science” or “data empowered learning” are used here, rather than “learning analytics,” since “learning analytics” comes with many connotations, and does not cover the full breadth of data activities and possibilities.

Though the university doesn’t have a campus unit responsible for learning analytics projects, there are a variety of resources available to instructors and academic departments.

University is in the process of implementing student data analytics software for predictive analytics and personalized education purposes.

We are just starting to look at these projects. There are a few individual research projects.

We have limited but somewhat decentralized learning analytics efforts. Learning Innovation, which is organizationally part of the Libraries, uses data from Sakai (our LMS) and associated learning technologies to inform decisions about usage and to optimize learning and the environments in which learning occurs. Learning Innovation also collaborates with other faculty and offices on research projects using our large Coursera course dataset with a primary focus on improving learning outcomes or optimizing courses. There are other groups exploring the use of analytics, but those groups are currently focused on creating policies and guidelines. For example, the Office of Assessment is involved with a Student Data Analytics Team looking at guidelines for access to data in our large ERPs (PeopleSoft, SAP, etc.).

While there are learning analytics projects (mostly led by colleges/departments, not campus-wide), the library is not currently participating in any learning analytics projects.

Answered No N=4

Not yet. We have been building the capacity to develop learning analytics and have revised our vacant Assessment/User Experience Librarian position to be heavily focused on Library Value initiatives, but at this point, we are not currently engaged in LA initiatives.

Nothing university-wide. Some individual colleges may have programs or pilots with no library involvement.

There is a campus group that is starting to look into using learning analytics to support student learning. Nothing formal, yet.

We have piloted a couple of projects relating to 1) library usage and demographics, but not success indicators (library) and 2) predictive analytics to develop statistical model related to student retention (Office of Undergraduate Education), but we have not yet initiated an institutional program.

2. **If yes, does your institution have a program/office that is responsible for learning analytics projects/initiatives?** N=41

Yes	29	71%
No	12	29%

If yes, please name the program(s)/office(s). N=26

Academic Planning and Institutional Research (APIR), Registrar’s Office, Vice Provost for Teaching & Learning (Assessment Division), Division of Information Technology (Highly distributed)

Assessment and Research, which is a division of the Office of the Vice Provost for Undergraduate Education.

Center for Assessment and Applied Research

Data Analytics

EAB Campus

Exists in three offices: Office of the Provost, The Institute for Teaching and Learning (TILT), and CSU Online.

I believe the university's Office of Budget and Planning is responsible for this work.

Institutional Assessment & Studies

Institutional Effectiveness & Assessment; Office of Research

Institutional Research & Information Management

Institutional Research, Assessment & Research in Division of Student Affairs, and Registrar all work on this.

Institutional Research, Planning and Assessment

Learning Analytics Research Network

Office of Assessment of Teaching and Learning

Office of Institutional Analysis

Office of Institutional Planning and Research (OIPR)

Office of Institutional Research (university), Assessment and Government Information (library)

Office of Institutional Research and Planning (OIRP), Division of Academic & Student Affairs (DASA), Distance Education and Learning Technology Applications (DELTA)

Office of the Provost and Information Technology Services

Office of the Provost, Vice Provost for Data and Information

Several offices are involved in learning analytics efforts at different levels.

The University Assessment Committee

The University Libraries are increasingly involved in assessment activities to better understand and demonstrate the impact of the Libraries on student outcomes. The Undergraduate Experience Initiative/ Office of the President was recently launched and the Libraries are partners in this effort.

Unizin Governance and Working Teams has a Learning Analytics cross-functional team. Other learning analytics efforts are decentralized in individual colleges. There is a Learning Analytics Informal Community of Practice.

UX & RIO

Within the library, there are several units responsible for and engaged in their own efforts for learning analytics, such as Data Management Services and Academic Liaisons (focused on learning and teaching). The Center for Educational Resources partners with faculty and graduate students to extend their instructional impact by connecting innovative teaching strategies and instructional technologies. Across the institution, analytics and assessment often are distributed in various offices throughout the university and medical campuses—so while various offices engage in these activities, there is no one, central office completely responsible for institutional assessment or analytics. This leaves some organizational analytics-based gaps that the Assessment and User Experience Department plans to help fill.

Additional comments N=4

Learning analytics is being done more in a collaborative way, rather than a centrally coordinated way at this time. Learning analytics activities initiate centrally and data reports are pulled from a central office of institutional research, but ad hoc data are requested as required by other initiatives. No formal program, charge, or assignment exists.

Not at the Libraries. The Learning Analytics Group (collaboration between the Associate Provost for Undergraduate Education and The Hub for Innovation in Learning and Technology) aims to coordinate and develop initiatives, but does not manage, oversee, or approve individual department, college, and administrative projects.

See above. Learning Innovation is often the starting point for learning analytics projects and initiatives, but Learning Innovation is not considered our centralized owner of learning analytics.

The Teaching & Learning with Technology (TLT) group is farthest along, but many groups are responsible for and involved in learning analytics initiatives, including World Campus and Undergraduate Education.

INSTITUTION DATA STORAGE

Note: Institutions use data warehouses, or a central set of databases, to aggregate and store data of interest This can include, but is not limited to, student data from systems like student information systems, student activities data, university budget data, and human resources data. People throughout the institution are given different levels of access to the central data warehouse based on their institutional needs for access to the data.

3. **Please indicate which of the following describes how student data is stored at your institution. Check all that apply.** N=51

Data is stored in a central data warehouse	41	80%
Data is stored by the office/department that collects it	38	75%
Data is stored in a separate learning analytics warehouse	9	18%
Data is stored in another repository	10	20%

Please briefly describe the other repository. N=10

Assessment and Research maintains separate files specifically for learning analytics analysis projects. This is not a formal repository, but rather a server space (via Box Entrusted).

Data is stored in many different systems across the library. Some data is stored in our ILS, other resource management tools for reserves, e-resources, and Inter Library Loan. Currently, working with our library IT, we've been developing a data store for assessment and analytics purpose. Other storage locations for staff are varied and include Spring Share, Google Sheets, internal networked drives, cloud-based storage options provided by the institution, on computer files, internal back-up drives, computer files, and sheets of paper (although the paper tallies eventually are converted to a computer file for reporting purposes).

Data is stored in several different databases. These serve different purposes based on how the data-points are usually reported.

Data is stored on a library shared drive, and in the case of one project by the GWLA consortium, data used for learning analytics is obtained from and stored by institutional research.

Intent is to utilize the Unizin Data Platform.

Planned, but not in place yet, in the Unizin repository.

Springshare and in UX files

Systems of record, the Student Information System, the Canvas LMS, etc.

The Library Technology Services Department securely stores our data.

The place student data is stored depends on the system the data is originating from. Data from Student Information Services and Systems (SISS), Sakai, and other individual component systems/tools often have different data agreements and are stored in different ways. Final grades, official rosters, etc. are only stored and managed by SSIS, for example. There is an effort underway to build a data warehouse that would provide access to many of these data in the same place, but this effort is currently stalled.

4. **If your institution has a warehouse/repository for aggregating student data, which unit/department is responsible for managing the warehouse/repository?** N=40

Administrative Services

Again, there is an effort underway to build a data warehouse that would provide access to many of these data in the same place, but this effort is currently stalled.

Central Information Technology (2 responses)

Central IT, also stored at the Unizin consortium, see http://unizin.org.

Computing Services and Systems Development

Division of IT and Registrar's Office

Enterprise Reporting and Analytics Services within Information Technology

Information Technologies

Information Technology Services

Information Technology; specifically, Business Intelligence

Institutional Research (2 responses)

Institutional Research, Planning, and Effectiveness

IRPA - Institutional Research, Planning, and Assessment Office

IT Services - Teaching & Learning

ITS and the departments that "own" the data.

Learning Analytics Data Architecture (LARC) // Office of Enrollment Data warehouse // ITS

Not sure.

Office of Academic Planning & Accountability (OAPA)

Office of Budget and Planning, Office of the Registrar

Office of Data Analytics

Office of Information Technology (OIT) (3 responses)

Office of Institutional Research

Office of the Provost, ITS, Office of the Registrar

Office of the Registrar

OIPR

Registrar's office

Registration and Records

Springshare

The Assessment & User Experience Department is the business owner of the repository. It is supported and developed by the Library Applications Group (IT).

The Office of Business Intelligence manages the data and the platform.

The technical aspect of our data warehouse is managed mostly by the university system IT (Administrative Information Technology Services) and campus IT (Technology Services).

University Business Intelligence

University Information Technology Services

University Information Technology (2 responses)

University Registrar

5. Please enter any comments you have regarding institutional data storage. N=12

A challenging environment, operationally and fiscally.

Campus is working towards a data stewardship model where roles are distributed across both units mentioned above [Division of IT and Registrar's Office].

Discussions on institutional data warehousing are taking place on campus.

General student data is stored in a central data warehouse. However, each department may perform their independent assessment projects, in which case the department will store the data they collect. There may be a separate learning analytics warehouse that the library is not aware of.

I don't have any knowledge of how these data are stored at the institutional level. The library has not been involved in any projects that would require access to those data.

It is my understanding that our student data is stored in PeopleSoft. The OAPA has been implementing analytics tools that interact with PeopleSoft.

Learning analytics is still nascent. Various units are collecting and using data, but efforts are not centralized under a single campus body, yet.

Purpose of this office as posted on its website: "The Office of Institutional Research, Planning, and Assessment (IRPA) provides essential information about the university for the purposes of decision-making, policy analysis, strategic planning, mandated reporting, and academic program review. We capture data on faculty, staff, students, and finances and use it to characterize the institution in quantitative ways using nationally accepted definitions."

Student data is aggregated into profiles and affiliation. Individual student data that would be identifiable in the data store is not retained. Personally identifiable data may still be found in the resource management tools for reserves and Inter Library lending, as well as in individual staff files. Data privacy is something we are working on addressing for operational data and library analytics currently. Current data management policy exists but is geared more towards researchers and Principle Investigators external to the library, although conversations are underway about developing a data management plan for library operations and analytics data. The Assessment and User Experience Department aligns our work with campus policy for IRB, HIPPA, and FERPA.

The university is currently in the infancy stages of implementing MyDay, a system dedicated to student, human resources, as well as financial data. Student data is the last phase to be implemented, and library data will not be included.

The university is very decentralized and data is stored in multiple ways.

University Learning Analytics guidelines have been drafted and are being adopted campus-wide, led by Interim Chief Information Security Officer/University Privacy Officer.

LIBRARY DATA COLLECTION AND RETENTION

6. Please indicate which of the following user data the library collects for its own learning analytics activities and whether that data includes identifiers. Check all that apply. N=46

User Data	Includes identifiers	Does not include identifiers	N
Reference service usage	5	37	42
Research consultations	13	29	42
Course-integrated instruction attendance	11	30	41
Workshop attendance	9	31	40
Physical collection circulation statistics	18	21	39
Attendance at other events (e.g., tour, orientations, etc.)	6	33	39
Database usage	8	30	38
Journal usage	8	30	38
E-resources usage (including eBooks)	10	28	38
Library website usage	2	36	38
Building usage	8	30	38
Instruction evaluations	5	33	38
Interlibrary loan requests	21	16	37
Library computer logins	12	19	31
Single sign-on login portals (e.g., LDAP, Shibboleth)	11	13	24
Security systems (e.g., security camera recordings)	0	23	23
Wifi usage	3	15	18
Other data	8	5	13
Total respondents	32	45	46

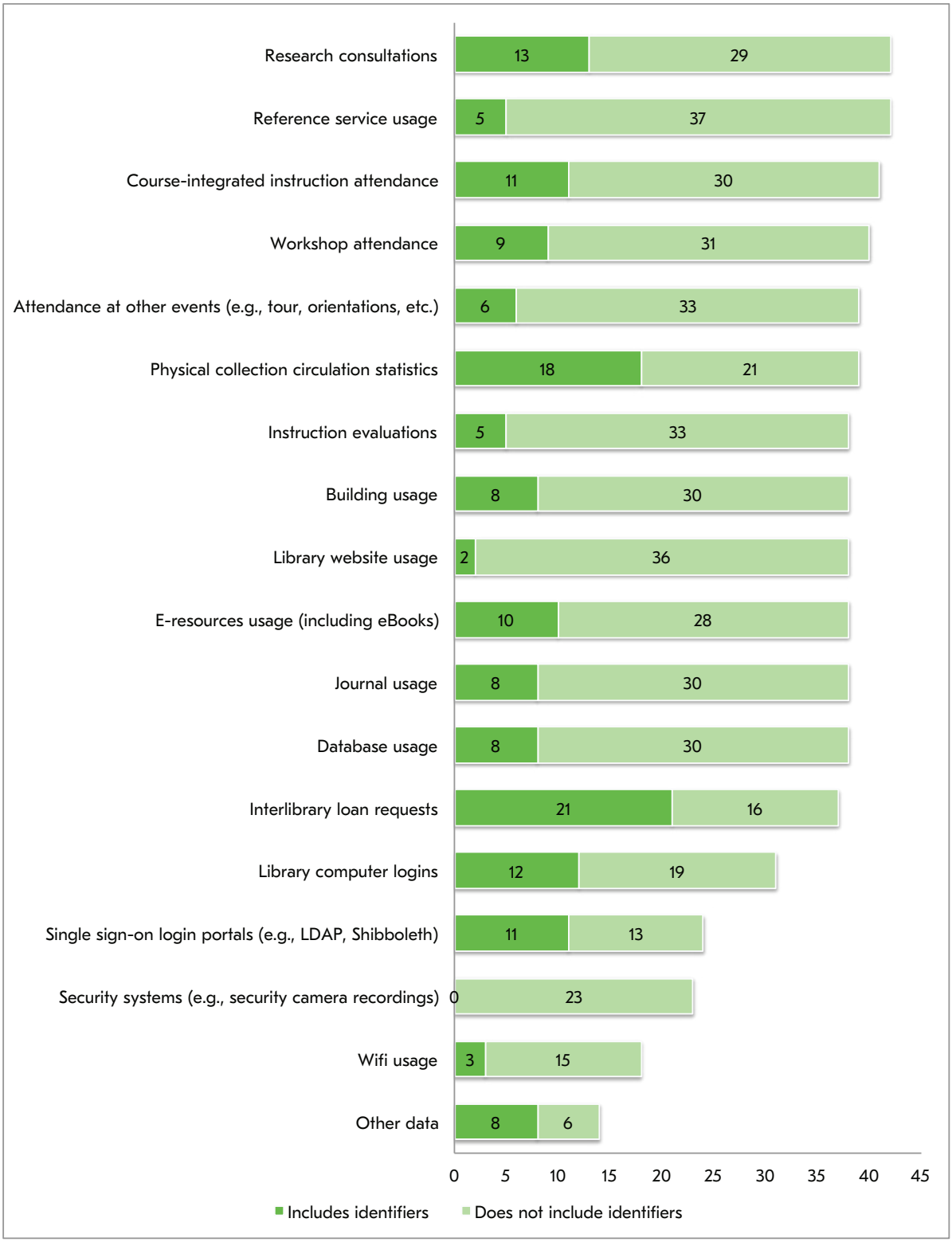
If you indicated that the library collects Other data with identifiers, please briefly describe that data. N=7

CANVAS (the LMS) usage data is collected and shared with the academic units, upon request. Note: Generally speaking, the Libraries collects data for improving the Libraries (collections, services, and spaces). We are not currently correlating library data with student outcomes, but we have plans to do so in conjunction with the university. This effort is currently in the planning phase.

Data from online modules used as a face-to-face instruction equivalent; data with identifiers is sent to course instructors for grading purposes, and de-identified versions are used within the library for analysis.

Qualitative data from library research studies; survey data; course assignment performance data.

Types of User Data Collected, With and Without Identifiers (N=46)



Springshare room reservations includes university IDs, which is an identifier. Customer Resource Management tools: currently this is a tool under investigation for the library, but it would potentially include identifiers, such as name, department, email.

We annually collect the above marked data, some of which may include identifying information at the time of the transaction such as ILL and reference. The identifying information is removed once they no longer are needed for business purposes. For the purpose of learning analytics, we don't keep identifying information collected through theses transactions. However, we conduct various assessment projects that may independently collect similar data with identifiers.

We have a graduate student use only floor in one library and it is restricted by students swiping/using their student ID card.

We have access to appointment data with identifiers for all students who make appointments with the Peer Research Assistants through WCOnline (writing center scheduling software). We also have an incomplete record of PIDs of students who use the service, which is available through the Student Data Dashboard. These are not entered consistently, though, so might not be useful for much.

If you indicated that the library collects Other data without identifiers, please briefly describe that data. N=3

Licensed e-resource use through EZProxy.

Use of videos created by the library, use of LibGuides created by the library

We collect analytics for e-resource and site usage without individual identifiers.

Additional comments N=11

Access to many of our systems requires a university computing ID but we do not collect that data for the library's purposes.

All of our circulation and materials usage require authentication but we do not retain those data after 30 days. To date, we have not used those data and there is some resistance to doing so in any capacity.

Building usage includes identifiers at times when card swipe is used (e.g., after normal business hours). Online reference service usage includes identifiers, whereas face-to-face reference service currently does not. Only a subset of instruction evaluations has identifiers. Access to many of our systems requires a university computing ID but we do not collect that data for the library's purposes.

Checked data types _CAN_ include identifying information (Unique identifier) depending on how query is constructed. Identifiers are used to aggregate data by user types and demographics, academic units. Data collected for websites and "services" like Springshare uses Google Analytics and is not ID'd to a level that allows association to an individual. No individual user identifiers collected for reference, consultations.

Data collected for websites and "services" like Springshare uses Google Analytics and is not IDed to a level that allows association at to an individual. No individual user identifiers are collected for reference, consultations.

Data comes in with identifiers, but they are not saved.

Data re: catalog use, item check out, electronic resource use, etc., do not report identifying info; at least not the reports that I've seen, anyway.

The majority of yeses above are managed and operated by central OIT.

There may be demographic, department, or status information available, but never personal identifiers.

These questions don't apply to us since our library is not currently participating in any learning analytics projects.

User university ID number is collected on most data with identifiers; if a user provides name and email on an email or in a chat reference session, this info is stored. Data re: catalog use, item check out, electronic resource use, etc., do not report identifying info—at least not the reports that I've seen, anyway.

7. Who participates in the collection of data used for the library's learning analytics? N=45

Librarians/library faculty	45	100%
Support staff	40	89%

8. Who participates in the analysis of data used for the library's learning analytics? N=45

Librarians/library faculty	43	96%
Support staff	29	64%

9. Does the library have a records retention schedule or other policy document that covers how long this data is kept? N=47

Yes	18	38%
No	29	62%

10. If yes, have data retention requirements been changed because of learning analytics? N=18

Yes	2	11%
No	16	89%

11. Please enter the amount of time (e.g., 5 years, 3 months, indefinite) library data that is used for learning analytics purposes is retained. N=28

Has a retention schedule/policy N=15

3

12 months

2 years for _SOME_ data (circulation, ILL, ...)

3 years

5 for paper

5 years

At least 6 years; in practice, often indefinitely

Based on the retention schedule, data is purged either 1-year, 3-years, when patrons become inactive, or after the transaction is complete, depending on the type of data.

Depends on level of data aggregation. Detail data (PID+usage ID)=1 month are kept for purposes such as tracking when a vendor shuts off an IP address.

Duration of the study for manually collected data, auto-collected data has different time periods.

If collected, per IRB requirements, 3 years.

Retention varies by specific type of data

Retention varies from 2 years (EZProxy logs) to 10 years (circulation records).

The retention varies by system.

Varies—Data with IDs: less than two years; without IDs: indefinite.

Does not have a retention schedule/policy N=13

Common practice is 3 years retention; there is no formalized retention policy in place.

Every several years, or so

Indefinite (8 responses)

Indefinitely

Varies greatly depending on the type of data and why it was collected

We automatically anonymize circulation data 30 days after an item is returned as long as there are no outstanding fines/fees. We clear from the Libraries' ILS all patrons who have been gone at least one year on an annual basis. We do not get rid of ILL patron data. There is no way to anonymize ILL data, and we'd lose all related transactions if we removed patron data.

12. **Please enter any comments you have regarding library data collection and retention.** N=22

All historical data not purged from systems. While data may contain personal identifiers, it is used in aggregate to count users and usage patterns for administrative and reporting purposes.

Although we do not currently have a data retention schedule or policy document, we are in the process of developing one and have reviewed our existing policies in order to be explicit about how data is used.

As noted earlier, the library doesn't engage in "learning analytics" per se, but it definitely engages in collecting usage statistics. With the exception of on-site professional training and ILL requests, identifiers are not used.

Circulation records are purged weekly.

Currently, we do not have a retention guideline that is specific to library records. However, we do have two general retention guidelines, the Administrative and Management Records guideline and Fiscal Records guidelines that apply to all university offices. These would apply to library administrative and financial records in lieu of a more specific guideline.

Data collection and retention is driven by external reporting needs as well as for specific decision-making related functions within individual units or departments.

Data collection varies across units, departments, and even librarian/instructor. We have not developed specific retention policies to govern learning analytics data collection because the data we are using for learning analytics is covered by existing categories in the data retention schedule.

I'm not certain it is accurate to describe use of the data as learning analytics. Various departments and libraries collect data. There is no comprehensive program to use the data in the way I think you are hoping to understand.

Identifiers are not included with on-campus usage of databases, journals, and e-books.

It is generally best practice to retain all information until it is no longer perceived to be needed.

Journal usage only includes identifiers when obtained via EZProxy System. Building usage only included identifiers when using card swipe system (only some areas). Studies with IRB approval will typically have data retention and destruction policies.

Library data retention follows university policy.

Library does not collect any data for learning analytics purposes.

Looked at only when something emerges causing attention to be refocused upon it.

Many data types are collected in the aggregate for reporting and may not be traceable to a specific user. Computer use data is collected by a non-library office.

State requirement

The Libraries' retention policy is currently under review and subject to change.

There is nothing explicit covering data collection and retention in terms of retention policy, but current thinking within the Assessment & User Experience Department is that we should follow the university record retention policy, in conjunction with developing our own internal data management plan.

These data are often available with the existing technology but are not collected in very useful formats and/or are not pursued based on cultural norms and long time library practice.

We have new library data community of practice that will discuss issues.

We separate personally identifiable data from specific item used. The two "streams" never come back together.

Working on a records retention policy is on our list for the summer, and we have only been collecting data for 3 years; I plan to advocate for keeping 3 years of data, so next year I expect that we will purge raw data from year one; data without identifiers that has been aggregated I plan to keep/display.

LIBRARY DATA SHARING

13. Does your library share any user data with other parts of the institution? Check all that apply.
N=52

Yes, to specific office(s)/department(s)	18	35%
Yes, to the central data warehouse	6	12%
Yes, to another data repository	2	4%
Yes, to the learning analytics warehouse	1	2%
Not yet, but we plan to in the next 6 months	3	6%
Not yet, but we plan to in the next 12 months	8	15%
No	26	50%

If your library contributes data to specific office(s)/department(s), please identify which one(s).
N=19

Aggregate numbers are sent to the Office of Institutional Research for IPEDS reporting.

Assessment and Research

CANVAS user data is contributed to the academic units, upon request.

Institutional Research for IPEDS reporting

Learning Commons partners, provost's office

Library fines are shared with the registrar's office.

Limited aggregated use data (for an academic department online program) was shared as a test.

Office of Assessment of Teaching and Learning, Office of Undergraduate Education, Department of English, College of Communication, Department of History

Office of Institutional Research, course-integrated instruction data is shared with local APAS system.

Office of Research, for annual reporting (ARL, ACRL, IPEDS/NCES) in aggregate with no identifiers.

Office of the Provost

OIPR, dean's office, Office of Academic Assessment and Institutional Effectiveness

OIT, so that identifiers can be married to the demographic data they maintain.

Provided to the instructors of the classes.

Provost's office and Institutional Research and Institutional Management, Office of Institutional Effectiveness

Research Office

Statistics on workshops & consultations to Graduate Studies & Post-doctoral Affairs

The library contributes aggregated data to the various academic departments, the Office of the Provost, the Budget Office.

We contribute data to the provost's office annually for both institutional goals and initiatives that the library and museums undertook. We also provide a libraries and museum dashboard of some key facts and operational usage data for the building, collection usage, research consultations, and instructional statistics.

If your library doesn't yet contribute data to the institution but plans to, please describe when that will begin, what data will be included, and where the data will go. N=10

A request for library data has been made by the provost's office. We are now in discussions about what data could be made available and to ensure that it is not going to be used for purposes contrary to ALA privacy guidelines.

A university-wide survey working group; Student Affairs; Office of Planning & Institutional Assessment. There is no slated time for when this process will begin, no specific data identified, and no specific location identified for the data at this time.

Currently, in collaboration with faculty in the School of Education, we are exploring how to map internal research collaborations among various academic departments both at our university and other peer institutions.

During re-affirmations, we share data with the SACS steering committee.

Institute for Social Research

Library consultation services may be included in the Learning Analytics initiative at the university.

Summer 2019: ILS data; ILL; database usage

These plans have not yet been determined.

Unizin Data Platform, but we don't yet know specifics of what they will want or what we will share. While we are willing to experiment, we do not yet know whether library data will be useful for institution-wide learning analytics purposes.

We are still determining what this will look like, but we are considering a combination of aggregate lending statistics, instruction attendance, and overall building usage.

Additional comments N=6

As far as we are aware, no one on campus has asked for any library-specific data beyond what was described in part one of this survey (related to data collected by Learning Innovation), and therefore we have not shared it. That said, institutional staff are beginning to express interest in having library-specific data related to how students are using library resources and services, so we anticipate being asked for data in the coming months/years. At this point, we do not have formal plans for how data will be shared. We do currently share results of aggregate analysis with other offices on campus when asked or when we feel other campus offices and units would be interested in the results of library studies or analysis.

As stated above, some of our Peer Research Assistant data goes to the Student Success Data Dashboard as part of the Engagement Centers initiative.

No plan to contribute library transactions data to the campus data warehouse. There is some interest but we don't have the capability.

The university does not have an institutional research office. There is a business intelligence unit, and there are some discussions starting with that team.

We are in contact with the office of student affairs to include library data in their analyses. No timeline has been set and no decisions about what data to include have been made.

We only share aggregated data with the Office of Assessment and Decision Support a couple of times per year. They collect IPEDS, Peterson Guide, and other types of high-level collections and budget figures.

14. Does the library place stipulations on how those units must handle the library's analytics data? N=33

Yes	8	24%
No	25	86%

If yes, please briefly explain the stipulations. N=8

All data is anonymized to protect personal information.

Circulation and ILL data are aggregated by department. Individual data is not released.

Library would not supply any data that would allow to identify what materials are used by individuals (e.g., books read, journals articles accessed, etc.)

Raw data is not provided. Reports and visualizations include aggregated statistics and summaries that include observations and recommendations. Currently, identifiers are not provided in the data we report or provide to others. In research projects, we often have to comply with the Institutional Research Board in order to protect privacy of students participating in assessment or UX projects.

There are very few cases that we share the data, but the data shared does not include patron information that it violates privacy.

We are in the process of developing these stipulations in a formal document; at this point, they are handled on a case-by-case basis.

We are in the process of making that determination.

We require completion of a data sharing agreement, signed by the researcher and the Associate University Librarian or Library Information Technology, that specifies the data requested, the specific uses it will be put to, and requirements around destroying/de-identifying any PII that is included in the specific data set.

Additional comments N=5

No, as data for annual reporting (ARL, ACRL, IPEDS/NCES) is in aggregate with no identifiers.

No, we don't share data.

They are more protective of the data than we are.

We do no currently have any stipulations in place. Other than CANVAS usage data, any data that we share has been anonymized.

We have not yet had the need because the few with whom we share have stringent regulations around what they collect and store.

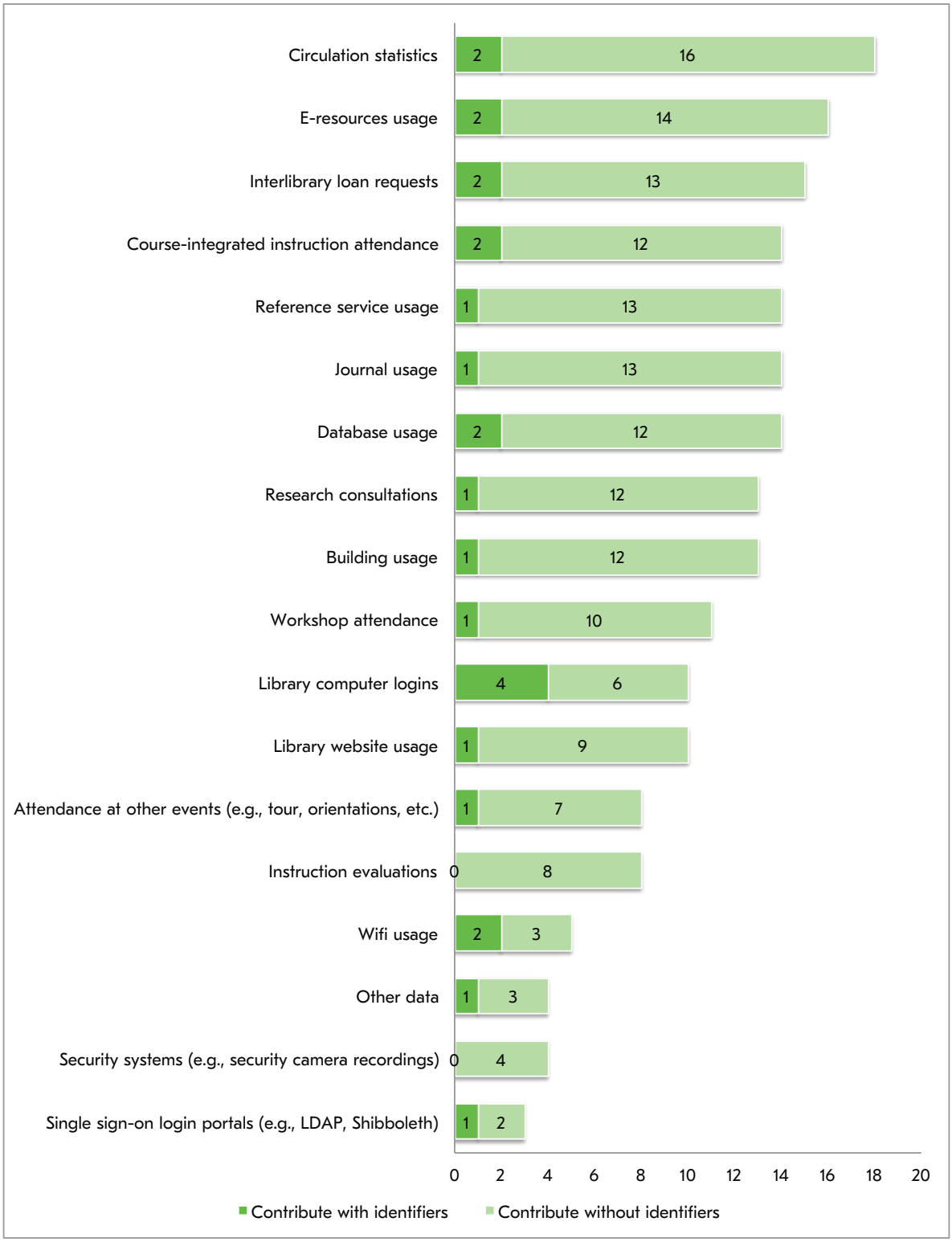
15. Are the stipulations codified in a formal document? N=8

Yes	2	25%
No	6	75%

16. Please indicate which types of data your library shares with other parts of the institution and whether that data includes identifiers. Check all that apply. N=24

Types of Data	Contribute with identifiers	Contribute without identifiers	N
Circulation statistics	2	16	18
E-resources usage	2	14	16
Interlibrary loan requests	2	13	15
Database usage	2	12	14
Journal usage	1	13	14
Reference service usage	1	13	14
Course-integrated instruction attendance	2	12	14
Building usage	1	12	13
Research consultations	1	12	13
Workshop attendance	1	10	11
Library website usage	1	9	10
Library computer logins	4	6	10
Instruction evaluations	0	8	8
Attendance at other events (e.g., tour, orientations, etc.)	1	7	8
Wifi usage	2	3	5
Security systems (e.g., security camera recordings)	0	4	4
Single sign-on login portals (e.g., LDAP, Shibboleth)	1	2	3
Other data	1	3	4
Total respondents	6	20	24

Types of Data Shared With Other Parts of the Institution (N=24)



If you indicated that your library contributes Other data with identifiers, please briefly describe that data. N=1

Student PIDs for students who visit Peer Research Assistants (as noted above, these are not entered for every interaction).

If you indicated that your library contributes Other data without identifiers, please briefly describe that data. N=1

Use of library created videos, use of LibGuides

Additional comments N=10

Again, we share data with a personal identifier (student ID) but no information on what book, article, database, etc. the person used.

Although we do not currently contribute any data with identifiers, we plan on doing this in the near future. Specific examples include research consultations, instruction attendance, workshop attendance, and other learning-related opportunities.

Budget information and volume counts to Institutional Analysis & Planning for KPIs. Library usage information during presentations about the library.

Building usage: yes, as door counts. Course-integrated instruction attendance: yes, aggregated instruction sessions of all types.

For annual reporting (ARL, ACRL, IPEDS/NCES) is in aggregate with no identifiers.

Security camera data is only shared with the campus police department as a result of an incident.

There are only a few cases we are sharing aggregate numbers with the university at this time.

These are total number counts. For example, total number of item circulations in a fiscal year, total number of reference and research consultations in a fiscal year.

We are not currently sharing any of this type of data.

We share summaries and data visualizations about use of library materials, workshops, and as part of curricular assessments (e.g., accreditation).

17. **If your library is not contributing all of its data to your institution, what are the reasons for not doing so? Check all that apply.** N=41

Privacy concerns	21	51%
Confidentiality concerns	18	44%
Resources (time, personnel)	16	39%
Lack of identifiers	8	20%
Bureaucracy	7	17%
Cannot collect appropriate data	7	17%
Cannot access data from different data sources	4	10%
Cannot provide data in formats required	3	7%
Other reason	23	56%

Please specify the other reason. N=23

As far as I know, the university has never asked for this data, except during re-affirmation periods.

As stated above, the university is not currently asking for library-specific data beyond that collected by Learning Innovation as described in part 1 of this survey. Again, we anticipate increased interest in library-specific data in the coming months/years and so are beginning to think about how we can collect, store, and share these data. We have no formal plans or process at this time.

Because assessment and data analytics are relatively new in our library, often others do not perceive the library as a place to obtain this type of data. This is slowly expected to change as our efforts at outreach continue across the libraries as well as across the institution.

Campus does not have a central data repository for data contributions.

Current data is shared as aggregate reports or for specific projects. As the campus implements learning analytics software we will provide most relevant data.

In general, I think the university tends to put less emphasis on data warehousing, analytics, big data, etc., when compared with its peers. I have a good relationship with the Office of Assessment and Decision Support, but their work does not involve learning analytics, only campus-wide surveys and demographic information about students. I have not seen any campus-wide efforts to mine student data for actionable findings, although I know that three years ago, when I started in this position, there was some effort to use "big data" at the university level. I think interest in that project has waned, and the leader of that initiative has moved on.

Institution is not requesting this data. No central learning analytics initiative.

It's not requested of us by campus units or leadership.

Lack of interest from institution or the library. Learning Analytics is piecemeal and silo-ed. Further, it's difficult to scale because the schools do not use a unified data structure and students can take classes within multiple schools.

Library data is not needed for current learning analytics efforts.

No clear objective that requires it and that would promise to bring value to offset resource investment.

No initiatives

No patron information is shared, only status and sometimes department, if possible.

Not requested.

Other than data required for institutional reporting, no data requested by other institutional units such as Office of Research.

Others on campus may not want the data or we have never been asked for it.

Our institution is very decentralized, and therefore we collect, store, and analyze our data based on various assessment needs within the library. Data may be shared with other parts of the institution on ad-hoc basis.

The library system is decentralized, making data collection a challenge. There is not a culture of strong data collection for the purpose of sharing in the libraries.

We are not entirely clear yet of campus needs and uses for library information.

We have no evidence that it would be useful to meet institutional goals in this area.

We haven't been asked to share this data with other university units, although we share selective data when we're addressing specific topics, such as the collections budget (e.g., database usage) or making a case for additional resources (e.g., building and equipment usage), etc.

We haven't had these conversations yet.

We need to analyze the data we've been collecting more closely before determining whether it makes sense to share the data. And, we have not had the personnel to help formulate a plan.

18. **In response to institutional learning analytics efforts, is your library collecting more, the same amount, or less data with identifiers?** N=43

More	15	35%
Same	24	56%
Less	4	9%

19. **How important is library data to learning analytics initiatives at your institution?** N=44

Very important	6	14%
Important	18	41%
Not important	20	46%

20. **How important is it to your library's administration to participate in learning analytics initiatives?** N=44

Very important	13	30%
Important	23	52%
Not important	8	18%

21. **Please enter any comments you have regarding library data sharing.** N=20

Although we are not currently doing so, our plan is to collect more data with identifiers in the near future in response to institutional learning analytics efforts and initiatives.

Although we haven't been asked to share our data systematically, we are expected to conduct assessment and collect data that support our strategic plan, its objectives, and metrics that show what we're accomplishing every year and how we're making an impact on the university's goals and objectives.

At this time, we have other priorities and limited resources.

If I thought I had birds of a feather at the university level, people who were interested in working with the library to pull in some of our data and track it alongside other metrics, I would be interested in testing out those waters, and I think library administration would be supportive of sharing some of our metrics. But by and large this is not a heavily data-driven campus.

Institution is not requesting this data. No central learning analytics initiative.

Learning analytics and library participation/sharing is becoming increasingly important with new budget models.

Learning analytics is important to my department, because we are responsible for instruction of information literacy and library skills, in all delivery formats. I do not feel that learning analytics is important to the library administration or university administration. They are more interested in quantitative data that can influence budgets, resources, etc.

Much library data is shared to external bodies and is public data, e.g., ARL, CARL, CAUBO.

Not a top priority at this time, but administrators have mentioned that it's a conversation we should be aware of.

Not yet on the attention level strategically for our institution. More of a required reporting activity.

Once the university implements the new integrated data structure, then more opportunities will open up for data sharing, and the importance of participating in the university's system may be heightened.

Share data on library's required information literacy course.

The Business Intelligence System is evolving to the point where data from the library could be incorporated. We expect to share more data in the future.

The Libraries are in early stages of participation in learning analytics and anticipates collecting more data in the future.

The library has not been seen as engaging in learning analytics, but this is an undertaking that is increasingly valued across the libraries, library administration, and the provost's office. There is some internal learning curve on how to best undertake this work, but it is exciting to see capacity and interest for this type of work growing across the libraries.

The library is interested in contributing to the success of the institution and our faculty and students. There are multiple challenges involved in moving in that direction, but work has started, slowly.

The library shares aggregate data with the institution to demonstrate our value. We do not contribute to an institutional data warehouse. We do not share identified data with the institution.

Useful/important for us to be involved in discussions, but we don't know whether our data itself will be useful.

We are just getting to the point where this is a priority; its not that it can't be done but we are in the process and there are various barriers that simply take time and evidence to change.

Within the Libraries, we are certainly interested in knowing more about how users are engaging with library resources and so have begun collecting more information. I also believe it's beginning to be important to the university that we collect and share library-related data. Up to this point, it has not been a high priority for the university to collect library data.

LIBRARY USE OF INSTITUTIONAL DATA

22. Does the library join/connect its data with institutional data via a common identifier for learning analytics purposes? N=48

Yes	13	27%
No	35	73%

23. Does the institution place stipulations on how the library must handle institutional data? N=40

Yes	28	70%
No	12	30%

If yes, please briefly explain the stipulations. N=27

All projects using patron data need to be approved by IRB. "Honest brokers" need to be used when connecting data points with individual identifiers.

All university data must be handled according to university-wide data management policies and procedures.

"All users of University information technology (IT) resources are required to use them in an ethical, professional, and legal manner." "Use of the University's information technology (IT) resources shall support the basic missions of the University in teaching, research, public service, and healthcare. Users of the University's IT resources are responsible for using these resources appropriately and respecting the rights of others."

Data is largely anonymized.

Data that includes identifiers must be kept on a certain platform and can't be shared but only with certain individuals.

FERPA laws are applied in the use of all such data.

Handling institutional data must comply with IRB and FERPA requirements.

Institutional data must be stored in such a way as to ensure that the data is secure and that access is limited to authorized users. Reference the university's data management policy for more information.

Institutional data requests happen on ad-hoc basis and depending on the type of information requested, we might be asked to follow certain protocols on how to store and use the data, especially if the data includes identifiers.

IRB approval

Just the usual stipulations around confidentiality and privacy. There is an information management policy.

Must be secure using standard computer security practices.

Personally identifiable information must be reported.

Privacy and security

Privacy restrictions

The Office of Information Technology requires an explanation of how data is to be used and limits access based on the use case.

The university stipulates that we cannot share data provided to us. Further, we must store that data on a separate, secured server.

These are handled on a per-project basis through the Institutional Review Board process.

These offices and policies cover stipulations, including Institutional Research Board, HIPPA, and FERPA.

Training is required to use student-level data. Student data is kept in secure server environments.

We are exploring what policies we would like to put in place in order to protect privacy and confidentiality and determine what information would be useful not only to share, but to receive back.

We are very limited in what we can acquire. Currently, we get patron status data and academic department only.

We have data-related policies at the central level for institutional data, and we must comply with those policies.

We have to honor FERPA and student/employee-initiated privacy blocks. We have to comply with the university's data sensitivity framework controls.

We provide a dataset collected using IRB approvals and this dataset is provided with requested data points and returned to the library. We anonymize the dataset and retain and manage it using FERPA and IRB requirements.

We regularly partner with Institutional Research. IR will not give us any institutional data unless we have conferred with IRB about the study and followed their protocols for approval/exemption. IR does not provide stipulations in a formal manner, but generally we must keep study participants' identities private. To directly email users and ask that they participate in studies, we need names/emails, which means that we are not able to receive truly anonymous data (receiving anonymous data would be the Libraries' preference).

Yes; the Office of Information Security places stipulations on all personal, confidential, and sensitive data.

Additional comments N=2

I assume that there would be stipulations if we collected identifiers as well, but we do not at this point.

The university aligns with relevant government regulations.

24. Please enter any comments you have regarding library use of institutional data. N=10

In the future we may explore linking certain library user data with institutional data for learning analytics purposes.

Institutional research provides de-identified student information that library instruction data is matched to based on course enrollment rather than attendance.

It is growing but very time consuming, as the library has few sources for usable data that are accessible at this time.

Occasionally use public information such as student FTEs. We may need to access personal data to resolve account issues.

See above. We often use data from Institutional Research to identify the demographics of students, faculty, and staff who use library services and resources or who participate in library studies (e.g., surveys, focus groups).

The library often obtains institutional data by request to Information Technology Services.

This is an area we hope to grow into in the future in terms of strategically streamlining library and institutional data where it makes sense, such as perhaps embedding the library into the early alert system for students.

We are not doing this yet.

We want to move in this direction.

We're looking at enrollment data for course related interactions and possible collections correlations in the future.

DATA PROTECTIONS

25. Please indicate which of the following data protections the library applies to its learning analytics projects. Check all that apply. N=40

Limit library staff access to raw data	39	98%
Remove direct identifiers from data (e.g., removing student ID number)	34	85%
Limit scope of data collection	31	78%
Technical security protections during data storage (e.g., encrypting datafiles in a cloud system)	26	65%
Physical security protections (e.g., locking up paper forms)	24	60%
Limit library staff access to analyzed data	24	60%
Delete data	20	50%
Limit data retention	18	45%
Technical security protections during data transfer (e.g., encrypting datafiles sent over email)	13	33%

Suppress data (e.g., removing data for groups smaller than 20)	13	33%
Other data protection measure	5	13%

Please briefly describe the other data protection measure. N=5

Access to data is limited to FERPA-certified staff.

Aggregate data as highly as possible across both collection usage and student profile information so that individuals are not identifiable.

Follow IRB guidelines for studies with people.

Most of our raw data is stored on secure active directories managed by the Office of Institutional Research. Again, data have a student ID but no identifiers on items used.

The library does not engage in "learning analytics" per se, but the techniques checked in the list above are used to protect circulation and on-site usage data.

26. If your library anonymizes its learning analytics data, please briefly describe the anonymization procedure. N=16

Data is anonymized by institutional research before it reaches the library.

Data provided as aggregate without identifiers. Identifiers purged from data two years after individual leaves university.

In presentation we only make available in aggregate.

Library data is typically presented in the aggregate.

Manual

OIT performs this function for the library.

Remove all ID numbers and names.

Removing the student ID number.

Strip personal information from data set.

University IDs are used only to associate data with aggregated user profiles and they are not retained in our systems or tools.

Use of "honest brokers" to link library and institutional data. Returned data for analysis is stripped from any identifying information. All subsequent analyses are carried out at cohort levels.

We are not currently anonymizing data, but we will be looking at demographics that define students in order to participate in program-level assessments and predictive learning projects.

We assign random numbers to individuals, and retain a key on an OIR server for use with longitudinal analysis.

We do not collect identifying information or IPs when we conduct surveys.

We mask identifiers for some of our data.

When we receive data from Institutional Research or other campus units/departments, we either request that data be anonymized before it is sent to us, or we anonymize it when we receive it. As described earlier, we anonymize circulation data after 30 days as long as there are not fines/fees associated with the data. Whenever possible, we anonymize data and use only unique identifiers to refer to user data.

27. Does the library have a data management plan for its learning analytics data? N=40

Yes	2	5%
No	38	95%

28. Please enter any comments you have regarding data protection. N=8

Different data management strategies have been used for different projects.

The Assessment Team has a data management plan.

The university does not currently have a data classification policy, which is often used to identify appropriate IT security for data stored electronically. Reference the Data Management policy for more information.

This will be a goal for the Assessment Librarian and Data Management Librarian.

We currently don't have a data management plan for learning analytics, but, we plan to do so.

We do not currently have a retention and deletion procedure, but will be developing one in the near future.

We follow certain procedures for managing our data, but have not recorded them in a formal data management plan.

While the library does not currently have a data management plan for library data, conversations and plans are underway to develop one within the next 12 months. The Libraries does have a privacy officer and our library tools and systems must comply with university privacy policies. Therefore, university policies around data protection should also extend to the library. There is a great deal of library material available about data management planning that has been mostly focused on external (to the library) researchers and principle investigators, but we're currently working to create a library data management plan for operational data and analytics. As stated earlier, analytics projects and work undertaken by the library's Assessment and User Experience Department to comply with IRB and other data privacy policies from the university.

PRIVACY POLICIES

29. Does your institution have a privacy policy? N=50

Yes	45	90%
No	5	10%

30. Does your library have a privacy policy that is separate from the institution's policy? N=50

Yes	31	62%
No	19	38%

If yes, does the library's privacy policy reference any of the following professional or legal documents? Check all that apply. N=29

University policies	20	69%
State/provincial laws on library records	19	66%
ALA Code of Ethics	17	59%
Terms of Service for software/application (e.g., Google Analytics)	13	45%

USA Patriot Act of 2001	9	31%
Family Educational Rights and Privacy Act (FERPA)	8	28%
Canada's Privacy Act	0	—
Personal Information Protection and Electronic Documents Act (PIPEDA)	0	—
Other document	3	10%

Please briefly describe the other document. N=3

ALA Policy on Confidentiality and Privacy of Library Records

California Digital Libraries commitment to user policy

HIPPA, Information Technology Policies—Electronic Information Classification

31. How often is the privacy policy updated or reviewed? N=27

Annually

Annually or as needed

Approximately annually

As needed (3 responses)

As the laws change and library stays in compliance on known policies.

Currently under review.

Every 3 years

Every 3–4 years.

Hasn't been updated since 2004.

I have no idea.

Infrequently

It is reviewed annually.

It should be noted that the institution privacy policy is brand new and in response to a new law requirement imposed by the European Union [GDPR]. That document was to be ready by June 1 but has yet to be posted.

It was updated this year. It is updated as needed and reviewed by both the University Library Dean's Council and General Council. There is not a set timeline for reviewing it, but it should be reviewed each time the website is redesigned, as well as any need for clarifying privacy policy that might emerge on an ongoing basis.

Last update of university policy 1/17, Libraries' policy 10/2013

No library specific policy.

Not sure. Last update was January 2018.

Periodically, but not on a regular cycle.

Periodically; undertaking review now.

Review cycle: every 2 years

The privacy policy is being discussed now at the university level to reflect institution's desire to use student data for predictive analytics projects. A group out of provost's office is tasked with developing guidelines and policy relating to the use of student personal data.

Typically once every few years and in response to new policy developments. Last update was in 2012.

Unknown

Varies

Yearly

32. Has your library's privacy policy changed in response to learning analytics initiatives? N=37

Yes	7	19%
No	30	81%

If yes, please briefly describe how it changed. N=5

Library does not have a specific privacy policy but our data handling is guided by state and federal laws and professional codes and guidelines.

Meaning that, the university-level privacy policy has changed in response to an environment that takes into consideration learning analytics, and the university-level policy will supersede the Libraries policy.

On occasion, with the Institutional Review Board (IRB) approval and with individual library user consent, the library may collect personal information to conduct user behavior research as part of our effort to continue enhancing our services.

Please see responses above, we are going to determine this information.

We created the "Responsible Use of Library Data" statement just prior to initiating the learning analytics project.

33. Do you inform students about your library learning analytics initiatives? N=43

Yes	18	42%
No	25	58%

If yes, after being informed about library learning analytics, do students have an opportunity to opt in or opt out? N=15

Can opt in	4	27%
Can opt out	5	33%
Can neither opt in or opt out	6	40%

34. Does the library obtain institutional review board (IRB) approval for its learning analytics initiatives? N=40

Yes	28	70%
No	12	30%

35. Does the library consult with university officials regarding the Family Educational Rights and Privacy Act (FERPA) and/or other similar legal requirements for its learning analytics work? N=40

Yes	24	60%
No	16	40%

36. Please enter any comments you have regarding privacy policies. N=13

All library staff are required to complete university-wide training on FERPA. The precise form of information/consent/opt-in varies by the project and the information collected. IRB approval has been sought and granted for project-based data collection.

Any data that we are gathering about student use of the library's resources, spaces, services, etc., is used for non-research purposes and within the library only.

Consult as necessary with general counsel and other administrative offices in the university depending on the nature of the project or initiative.

IRB approval gained if needed; not always needed for internal review purposes. Google analytics is running on our sites; students don't have the opt-in/opt-out option for those analytics. Our public services staff are trained on patron privacy and confidentiality.

Not at the moment, but we are taking all of these options into consideration.

On the advise of our APIR data analytics is for process improvement, not research subject to IRB restrictions.

The Libraries does not have learning analytics initiatives.

The library protects the privacy of its users. Library employees have no expectation of privacy in using library resources/collections or systems.

The university level privacy policy will supersede any library or departmental level privacy policies developed.

We consult with IR, the IRB, internal library legal experts, and the university's general counsel when we are beginning a new assessment/learning analytics endeavor. Our process for seeking advice/counsel depends on the scope of the study.

We don't additionally inform students for general data collection beyond the university's disclosure policies. However, for many studies involving more detailed and specific data (e.g., performance on assignments) we obtained signed consent.

We inform students about some learning analytics initiatives, particularly those that involve identifiers. These projects provide the option to opt out. These projects are subjected to IRB review. Other data is simply analyzed without identifiers.

We only consult and obtain approval from IRB if we intend to publish or present the results of our learning analytics to individuals outside our organization. If the data collection is solely for organizational development purposes, we do not seek IRB approval, however we still make every effort to adhere to IRB participants' privacy protection protocols.

PROCEDURES

37. Does your library have any internal staff documents or guidelines that inform your learning analytics initiatives? N=44

Yes	11	25%
No	33	75%

If yes, please briefly describe the contents of the document. N=9

Definition of performance indicators, process for reporting data and trends

It's not just about learning analytics; it is our Statement on Data Use for Library Assessment Purposes, and it covers data that we collect about librarians too.

Library Assessment website

Prepared and maintained in UX

Project plans for scoping of data analysis for research question determined by library.

Through past training led by staff and consultants around data analytics, assessment, and data visualization. Also, there have been outreach efforts such as providing access to webinars around visualization or data privacy in order to have a better conversation related to these topics across the organization. Some of these efforts are documented on the wiki. Overall, most of the current learning analytics initiatives are being guided by an internal planning document that is a strategic plan developed by the Assessment and User Experience Department. This plan outlines strategies for building capacity in learning analytics, data visualization, user experience and overall assessment.

We have a document that specifies who can access which data sets (raw data, anonymized data). Distribution of the data is approved by the university librarian or other appropriate administrator.

We have an assessment plan.

We have policies relating to collection, storage, and access to data as well as levels of aggregation and reporting. All projects are cleared through university's IRB process.

38. Does your library have a process in place for handling institutional data requests (e.g., If campus IT requests information on study room reservations)? N=45

Yes	15	33%
No	30	67%

If yes, please briefly describe the process. N=13

All ad hoc responses

All requests are brought in for discussion/decisions to the Library Management Team.

All requests come to library administration. FERPA data release must be approved in writing by the registrar. Third party software is reviewed and legal agreements executed before LTI integrations are approved.

Escalate to library administration for approval before sharing with other campus entities.

Information requests usually come to an associate dean and are handled, with assistance, through their office.

It must go through the Department of Assessment and Government Information.

Libraries' privacy policy informs responses to requests for data.

Most requests are referred to the OIPR; however standard library surveys are routed to the assessment librarian.

Our Library Reporting and Assessment Analyst handles regular institutional requests related to KPIs. Out-of-the-ordinary requests would be sent to the library executive.

Requests are made known to the Dean of Libraries and the path forward is discussed with appropriate stakeholders.

Requests are reviewed by the appropriate division and approved by the University Librarian before data is shared.

Requests are routed through the assessment and statistics coordinator, who determines how to respond and gathers data as needed

We apply our standard privacy policy.

Additional comments N=5

I don't think we generally have received these types of requests.

Not a formal process. The person listed as responsible for collecting and keeping the data is contacted and is responsible for responding when data requests are received.

The institutional request for data has prompted us to begin this analysis and discussions.

We would cooperate and collaborate with any department requesting institutional data.

While there is not currently a plan in place, these types of requests would likely be routed to the appropriate people if they came into the library as a request from another office. To my knowledge, no other campus partner has requested this type of data from us yet, but it would be good to have a workflow in place in case this does happen in the future.

39. What types of training have library staff received to support library learning analytics projects? Check all that apply. N=43

Training on specific tools	29	67%
Institutional Review Board requirements	27	63%
Privacy requirements (e.g., FERPA)	22	51%
Data visualization	20	47%
Data management	17	40%
Data security	15	35%
Anonymization practices	9	21%
Data cleaning	8	19%
No training	7	16%
Other training	6	14%

Please specify the other training. N=6

Creating protocols for user surveys. Staff can consult with our library reporting and assessment analyst.

Library staff have expertise in many of these areas but have neither received nor been required to participate in formal training offered by the university or other entity.

Research analytics

Research methods

Statistics (a little)

We will likely need more training as we begin to consider what data to share, policies, etc.

40. Please enter any comments you have regarding learning analytics procedures. N=7

All are trained on FERPA by the university. Training on other topics varies by staff member and project.

Currently our learning analytics are informal, ad hoc user assessment. Usually anonymous and qualitative.

Our efforts at learning analytics are growing, but relatively new, so sometimes procedures may be a bit lacking related to analytics—but this is something that should be articulated and documented.

Procedures are carried out by staff across multiple departments across the libraries.

The assessment analyst has training on all the above marked items. We have not provided official training for other staff beside IRB required trainings. However, the assessment analyst provides consultations on majority of learning analytics projects to ensure adherence to best practices.

The library hires staff with training in all these areas to conduct learning analytics projects.

We do not have a formal process for handling data requests, but these requests would be reviewed for privacy implications before data is provided.

LEARNING ANALYTICS PARTNERS

41. Is your library currently working with consortia that are building capacity for learning analytics (e.g., Unizin, University Innovation Alliance, regional consortium, etc.)? N=49

Yes	16	33%
No	29	59%
No, but our institution is currently working with consortia	4	8%

If yes, please specify which one(s) and the nature of the work. N=14

Greater Western Library Alliance (GWLA)

GWLA Student Success initiative as an example of us contributing data to broader projects.

GWLA, study to understand how libraries contribute to student learning.

Statewide learning analytics initiative. Unizin member.

The Ivy League Libraries (Borrow Direct)

Through GWLA

Triangle Research Libraries Network (TRLN): TRLN institutions are interested in collecting aggregate usage data of library resources in order to analyze cost per use and determine how users are engaging with consortial resources. Ivy Plus Libraries (IPL): as with TRLN, the Ivy Plus Libraries are interested in collecting aggregate usage data of library resources in order to analyze cost per use and determine how users are engaging with consortial resources. We are also interested in gathering consortial data in order to negotiate pricing with library vendors. We have also worked with IPL partners to develop and explore innovative ways to collect and use aggregate user data. We are the beginning stages of this, but IPL partner libraries are interested in combining resources and expertise to build capacity for learning analytics projects that would be of use to all 13 IPL libraries (and beyond IPL, too).

University Innovation Alliance. Have initiated an Educational Advisory Board Student Success Collaborative. Also Monitoring Advising Analytics to Promote Success (MAAPS).

Unizin (2 responses)

Unizin, IMLS grants

Unizin advisory committees

Unizin, and some with Barnes & Noble. With Unizin, we are collaborating on a data platform using a common data format, specifically linked to the Canvas LMS.

Unizin's common data platform

42. Does the library partner on learning analytics initiatives with any campus units for learning analytics initiatives? N=48

Yes	18	38%
No	30	62%

If yes, please specify which one(s) and the nature of the work. N=17

Academic Technology Services (ATS) is a division within the Libraries. ATS is responsible for administering CANVAS, the library's LMS. Out of the box, all instructors can see course-level analytics for the courses they teach. ATS has partnered with some academic programs to correlate this general usage data specifically for instructional design and program improvements. This is not "learning analytics" proper, nor a specific initiative as alluded to in the question, but perhaps worth mentioning. These programs include the School of Theology DMin program and the School of Public Health EMPH program.

APIR: we provide data visualizations about course related library instruction interactions. Departments: we develop e-learning micro-courses that create learning data that is co-shared.

Assessment and Research: quantitative statistical analysis and modeling of data.

Campus units we partner with include Institutional Research (IR), Office of Assessment, Social Science Research Institute, Registrar, Student Information Services and Systems, and the Office of Information Technology. We partner with these units and departments in order to match data they have about library users with data collected in library systems. We use and analyze these data in order to learn more about how students, staff, and faculty are using library services and resources and to make improvements to existing services and resources. We also analyze usage data to understand more fully how resources (e.g., online journals) are being used, relative to costs.

In past we have partnered with School of Humanities and Writing Center to assess the effectiveness of our Research Consultation Services.

Institutional Effectiveness

Joining the EAB campus initiative, along with Learning Commons partners.

Office of Assessment of Teaching and Learning, Office of Undergraduate Education, Department of English, College of Communication, Department of History

Office of the Provost

Office of the Provost for Learning Commons usage

Provost Office: data collection. School of Engineering, Office of Deputy Dean for Academic: regression analysis of factors influencing GPA among undergrad engineering students.

Unizin Governance teams, Learning Analytics Cross Functional Team, College of Liberal Arts, Information Systems, Office of Institutional Research

We are exploring harvesting data from wifi logs and EZProxy from the IT Security unit.

We plan to pilot sharing some library use data with Undergraduate Studies to use in their predictive model for student retention.

We share data and work with the Office of First Year Studies and the Office of Faculty Affairs relating to classes taught by and through the Libraries.

Yes for research analytics and also the library has some involvement and participation into a campus-wide initiative called Student Services Excellence Initiative (SSEI). SSEI is a multiyear, university-

wide effort to improve the experience of students by refining administrative procedures and updating/streamlining the student experience across the university.

Yes, just started partnering with the Division of Academic & Student Affairs to share data around student use of space and services in a new Academic Success Center in the Libraries, and to share expertise and potential methodologies for investigating the impacts of library use.

Additional comments N=3

Again, while we do not currently partner in this way, we plan to in the near future.

No, except with OIPR, from whom we get aggregated student data.

When we did an Assessment in Action project (before my time), I think we partnered with someone from IT Services, Teaching and Learning, and also from the Neighborhood Student Success Initiative.

ADDITIONAL COMMENTS

43. Please enter any additional information regarding learning analytics activities at your library that may assist the authors in accurately analyzing the results of this survey. N=14

Because the university is in its infancy with learning analytics, so are the University Libraries. Beyond some stats collected in regards to instruction/workshop/research consultation attendance, we don't collect much data in this arena. The university analyzes student portfolios and writing samples, but this data is rarely shared with the libraries, and we are not connected to it in any way. The librarians do informal assessments, but nothing robust enough to categorize as a "learning analytics initiative".

Current learning analytics work is tied to the First Year Studies program and a few other required courses with a major library component. Past projects have been more all-inclusive, and future work will likely be expansive.

Generally speaking, the Libraries collects data for improving the Libraries (collections, services, and spaces). We are not currently correlating library data with student outcomes, but we have plans to do so in conjunction with the university. This effort is currently in the planning phase.

I think it is fair to say the library is in the very beginning stages of considering how to engage in learning analytics. We are very interested in the results of this survey, and of learning more about how to move along the path.

"Learning analytics" efforts still nascent at the university, but foundations are being laid. At this stage, efforts are not coordinated across campus units but there are beginnings. The Libraries are beginning by analyzing usage trends by types and patron groups across academic units to inform resource allocation and outreach activities.

Most of the questions do not apply to our library and have been left blank. We have supplied responses to what seem relevant.

My library is trying to catch up on collecting appropriate data for analysis. We're ahead in some areas (journal use, circulation, etc.) but behind in others (assessment of learning outcomes). We tend to rely on our data collection tools to do the storage and management for us (we use LibInsight, which is a relatively newly acquired tool. Before that we were using spreadsheets stored in Sharepoint). It's difficult to get buy-in from librarians and staff members to report. We can only work with the data we have. I also find that the privacy concerns beyond FERPA no longer serve us well as a library. How are we supposed to show that students who have multiple contact points with the library across their undergraduate time do have improved retention, graduation rates, GPAs, etc., if we cannot link those

contact points (check outs, journal use, study room booking, research consultation scheduling) with students and categorize them into groups or cohorts? It's not possible.

One note regarding our institutional data collection; the library is planning to join the university EAB initiative, however we haven't joined yet.

The Libraries are not involved in learning analytics at this time and has no immediate plans to do so.

This is an emergent area of practice. As we develop strategies to move forward, we are aligning to university policy and procedure. We expect this area to further develop over the next year. We are participating with efforts such as Unizin and IMLS grants to further our infrastructure policy framework and practices.

We are implementing a new business analytics system, and are exploring how, and how much, to get the Libraries integrated into this environment.

We do instructional assessment for our own use to assess effectiveness. Ethics approval is not usually required for internal service assessment. We have a library data community of practice where data discussions can take place. Google analytics runs on our websites.

We feel that it IS possible to participate in institutional initiatives that improve the experiences and outcomes of our students without compromising student privacy or our professional ethics. Although we value our ability to contribute to learning analytics discussions on our campus, we will not contribute data to learning analytics unless there is evidence that the data we can provide will make a positive difference for our students.

While we are aware of and very interested in library value research, it was not clear how the Siemens definition and library as value relate to the survey questions—as some questions were very broad, while others were focused. It was also not entirely clear in every question if institution referred to the library or the university, so we interpreted it sometimes as the library, and other times as the university depending on the answer we provided. Lastly, in most of the answers, we did not include the assessment initiatives of the Center for Educational Resources, as it has different goals and practices in place for analytics that are separate from the library even though administratively housed in the same building and sometimes aligning on outreach, initiatives, and goals.

Responding Institutions

University of Alabama
University at Albany, SUNY
Boston College
Brigham Young University
University of Calgary
University of California, Irvine
Case Western Reserve University
University of Colorado at Boulder
Colorado State University
Cornell University
University of Delaware
Duke University
Emory University
University of Florida
Georgetown University
University of Hawai'i at Manoa
University of Houston
University of Illinois at Urbana-Champaign
Indiana University Bloomington
University of Iowa
Iowa State University
Johns Hopkins University
Library of Congress
Louisiana State University
University of Louisville
University of Maryland
University of Massachusetts, Amherst
University of Miami
University of Michigan
Michigan State University
University of Minnesota
University of Nebraska—Lincoln
New York University
North Carolina State University
Northwestern University
Ohio University
Oklahoma State University
University of Oregon
Pennsylvania State University
University of Pittsburgh
Rutgers University
Syracuse University
Temple University
University of Tennessee
Texas Tech University
University of Toronto
Vanderbilt University
University of Virginia
Washington State University
Washington University in St. Louis
University of Waterloo
Western University
University of Wisconsin—Madison
Texas Tech University
University of Toronto
University of Virginia
Virginia Tech
Washington State University
University of Waterloo
Western University
University of Wisconsin—Madison

Representative Documents

Library Privacy Statements and Policies

UC Irvine Libraries Privacy Statement

Last updated: *August 17, 2004*

The UC Irvine Libraries provide the Libraries Web site and services to facilitate the pursuit and production of knowledge in support of learning and scholarship at the University of California, Irvine. Your privacy while using the UC Irvine Libraries Web site and services is an important element of intellectual and academic freedom. UC Irvine Libraries are committed to protecting the privacy of our library users. Our policies also support the California Digital Libraries commitment to user privacy and the precepts of confidentiality described in the Code of Ethics of the American Library Association , which states: "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted."

Confidentiality of Library Records

In the course of providing services, such as Library Search, Interlibrary Loan, and reference services, the Libraries acquire personally identifiable information about you, including your name, university ID, and items borrowed. When it is necessary for the Libraries to identify users in the course of normal library business, it is our goal to keep personal information for the shortest amount of time necessary to complete transactions or provide service. Access to personal information is restricted to authorized library staff who need it to conduct library business. Personal information is never revealed to external parties unless required by law and never used for commercial purposes. The Libraries adhere to the UCI Guidelines for the UC Electronic Communications Policy, campus and UC policies, and state and national laws.

Library Search

In order for the UCI community to conduct business with the Libraries (e.g., library circulation records, "My Library Account" portal service, interlibrary loan requests), the Libraries maintain a patron database in the Library Search that stores personal information. Transaction records are deleted from the Library Search system after each transaction is completed. Inactive patron records are periodically removed from the patron database. The Libraries use the information in your patron records only to interact with and provide service to you (e.g., fulfilling interlibrary borrowing requests, placing holds, and collecting overdue fines). Browsing Library Search to look up titles and check book and journal locations does not require any personal information from you.

UC Irvine Libraries Web Site

The UC Irvine Libraries routinely collect information to help us manage the site and improve service. Examples of such information collected and stored by the UC Irvine Libraries Web site include:

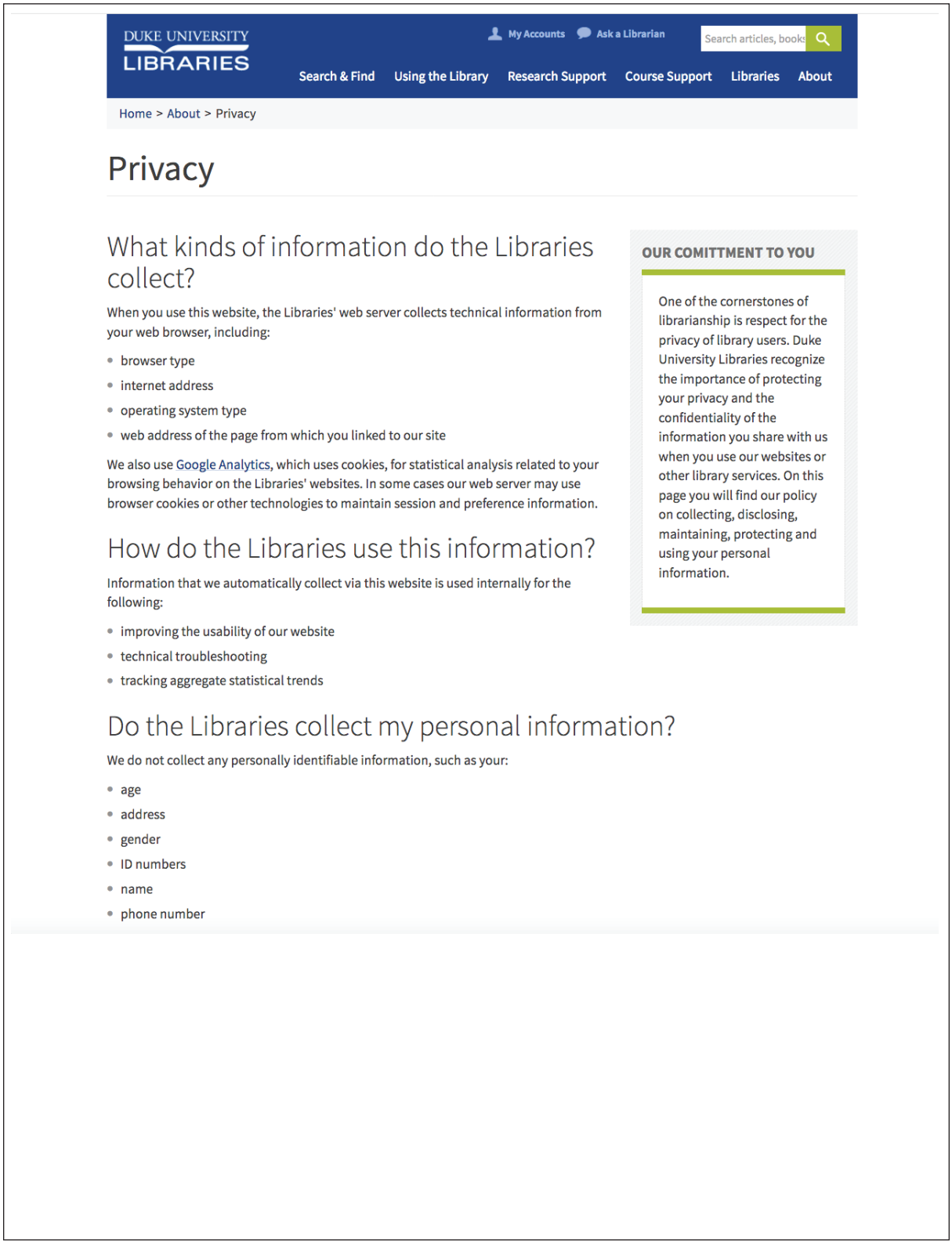
- your Internet location (Internet domain and IP address)
- type of browser and operating system used to access our site
- date and time our site was visited
- pages visited on our site
- search terms used on our search engines

The UC Irvine Libraries Web site links to other sites and resources that are not under the administrative control of UC Irvine Libraries. These external sites may have privacy policies that are different from UC Irvine Libraries or none at all. UC Irvine Libraries cannot guarantee the privacy policies of these sites. Where the Libraries contract with vendors for digital information products and resources, every attempt is made to include user privacy protections in the license agreements. Often you can tell you are leaving a UC Libraries Web site by noting the URL of the destination site. We encourage you to read the privacy statements at these sites to determine their privacy practices.

Related Policies

- User Rights and Responsibilities
- Ask a Librarian Privacy Statement

DUKE UNIVERSITY LIBRARIES
Privacy
https://library.duke.edu/about/privacy



DUKE UNIVERSITY LIBRARIES

My Accounts Ask a Librarian Search articles, books

Search & Find | Using the Library | Research Support | Course Support | Libraries | About

Home > About > Privacy

Privacy

What kinds of information do the Libraries collect?

When you use this website, the Libraries' web server collects technical information from your web browser, including:

- browser type
- internet address
- operating system type
- web address of the page from which you linked to our site

We also use Google Analytics, which uses cookies, for statistical analysis related to your browsing behavior on the Libraries' websites. In some cases our web server may use browser cookies or other technologies to maintain session and preference information.

How do the Libraries use this information?

Information that we automatically collect via this website is used internally for the following:

- improving the usability of our website
- technical troubleshooting
- tracking aggregate statistical trends

Do the Libraries collect my personal information?

We do not collect any personally identifiable information, such as your:

- age
- address
- gender
- ID numbers
- name
- phone number

OUR COMITTMENT TO YOU

One of the cornerstones of librarianship is respect for the privacy of library users. Duke University Libraries recognize the importance of protecting your privacy and the confidentiality of the information you share with us when you use our websites or other library services. On this page you will find our policy on collecting, disclosing, maintaining, protecting and using your personal information.

But what about personal information I submit via a web form or an e-mail message?

We interact with our library users regularly and receive personal information via email messages, chat sessions, web forms and other communications. If you submit personal information via one of these platforms, we:

- use your information for the purpose for which you submitted it only
- will not use your personal information for any other purpose
- will not combine your personal information with the other types of information we collect
- do not disclose to third parties any information that could be used to identify you or your use of Duke University Libraries resources, except as required by law or appropriate law enforcement procedures

What about the personal information in my online library account?

The Duke University Libraries maintain personally identifiable information in the online accounts of valid library users. For example:

- We receive personal information from the Registrar's Office (for students) and from Human Resources (for employees) in order to create and update the library accounts of users affiliated with Duke University.
- We obtain personal information about you in order to create your library account. We will maintain the confidentiality of all information we seek or receive and of the materials you consult, borrow or acquire — such as information related to circulation records; database search records; Interlibrary Request records; Duke University Libraries facilities, materials or services and reference interviews.
- We collect and store personal information you submit via the Libraries' web-based management tools — such as forms related to asking reference questions, requesting and renewing books and saving search histories or resource preferences. We use this information to maintain your library account and to provide services to you. We do not make this information available to any other entity outside the Libraries, except as required by law or appropriate law enforcement procedures.

Can I disable cookies and other tracking technologies?

Yes. You can disable cookies and other web technologies in your browser preference settings. However, please keep in mind that doing so may mean some features of this website will not function properly.

What are the privacy practices of the third-party tools the Libraries use?

Our website contains links to websites and licensed databases that Duke University Libraries does not maintain or support. We use third-party tools for some of our library services (such as online chatting with a librarian and searching for materials via specialized widgets). Please note that Duke University Libraries is not responsible for the privacy practices or the content of these third parties. We encourage you to read the policies associated with these third-party tools before using the tools.

Can I see the information maintained in my library account?

You are entitled to view your library account information and to amend information that is incorrect.

- If you are a student, you can correct your library account information via the Registrar's Office.
- If you are a Duke University employee, you can correct your library account information via Human Resources.
- If you are a patron who has purchased borrowing privileges and who shows proper identification, you can correct your library account information at the library that issued your library card.

Is my information secure?

In general, Internet transactions are not secure because they often are not encrypted. In some cases, however, transactions on our website occur using a SSL (Secure Socket Layer protocol) connection. This provides increased security to the information as it is transmitted. Only authorized library staff with assigned passwords may access personally identifiable information stored in Duke University Libraries' computer systems, and they may do this for the purpose of performing library work only. We use industry-standard security measures to protect any personal information that you may provide to us. However, we cannot guarantee that your submissions to our website, any content residing on our servers or any transmissions from our server will be completely secure.

How will I know if this privacy policy changes?

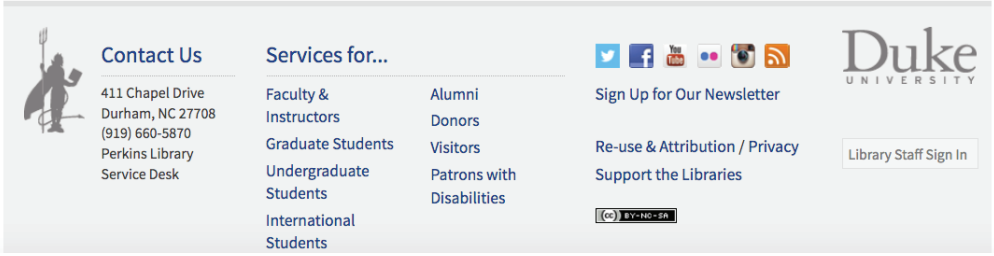
We will post any substantial changes in this privacy policy at least 30 days prior to the change taking effect. Any information collected under this current policy will remain bound by the terms of this privacy policy. After the changes take effect, all new information we collect, if any, will be subject to the revised privacy policy.

How can I get more information about this policy?

If you have questions about this policy or feel that we have acted in violation of this policy, please contact the webmaster.

Any other information I need to know?

- Duke University Libraries also adheres to Duke University privacy and computer policies published by the IT Security Office and the Office of Information Technology.
- The American Library Association provides information about the privacy and confidentiality principles supported by the library profession.



Robert W. Woodruff Library

Policy on the Collection, Use, and Disclosure of Personal Information

(Rev. 23 August 2013)

Introduction

Emory University Libraries recognize the importance of freedom of speech and of personal privacy of students, faculty, and other users of the libraries' materials. We endeavor to ensure the privacy of our users' communications, whether by face-to-face, telephone, email or other electronic means.

Use of library facilities whether in person or via computer may produce personally identifiable information (information which can be directly or indirectly tied to a specific person).

Access to personally identifiable information[1] is restricted to Library staff who need it to conduct Library business[2]. Personally identifiable information is never used for commercial purposes and is never revealed to a third party except as required and authorized by policy, law or to comply with a subpoena or court order only with the consent and advice of the University's Legal Counsel. The Library is supported in these practices by national, state and local laws, as well as by University policies.

Except as required by law, users of Library systems and services are informed whenever personally identifiable information other than transactional information will be collected and stored automatically by the system or service. The Libraries retains personally identifiable information only so long as it is required for operational purposes.

The Library does not routinely inspect, monitor, or disclose records of electronic transactions for other than Library business purposes. The Libraries and University Policies prohibit employees and others from seeking out, using or disclosing such information without authorization, and requires employees to take necessary precautions to protect the confidentiality of personally identifiable information encountered in the performance of their duties or otherwise.

Library Web Sites

In the course of providing you with Web-based services, The Library collects and stores certain information automatically through our Web sites. We use this information on an aggregate basis to maintain, enhance or add functionality to our Web-based services. It includes:

- your Internet location (IP address)
- which pages on our site you visit
- the URL of the Web page from which you came to our site
- which software you use to visit our site and its configuration

This type of data is not personally identifiable.

Links to External Websites

The various University Libraries' websites link to Internet sites and services outside the administrative domain of the libraries. Emory University Libraries does not govern the privacy practices of these external sites. Users should read the privacy statements at these sites to determine their practices. When one or more of the Libraries contracts with vendors for access to online content, such as journals and databases, every attempt is made to include user information protections in the license agreement.

Cookies

A "cookie" is a piece of plain text stored on your computer by a web server and used primarily to customize your interaction with the web. Some cookies last only for the duration of the session, while others are persistent and reside on a computer's hard drive until the user deletes them or the computer is refreshed. As a matter of policy, cookies are erased from Emory University Libraries' public computers periodically throughout the year and at the beginning of each term.

Web Analytics

Emory University Libraries use web analysis tools, including Google Analytics, to capture and analyze web statistics. Google Analytics is a cookie-based analytics program that uses cookies to track website activity. The Libraries also maintain local logs of web activity for statistical assessment using Webalyzer and other log analysis tools. These tools, including Google Analytics, typically collects, the following information: Network Location; Hostname; web page(s) requested; referring web page; browser used; screen resolution; size of data transferred; date and time. No personal information is stored within cookies. Cookies can be disabled within a browser's preference or option menu. For more information about Google Analytics, see Google Privacy Center - Privacy Policy.

Accessing Personally Identifiable Information for Other Than Library Business Purposes

The Library shall only permit the inspection, monitoring, or disclosure of personally identifiable information for other than Library business purposes: (i) when required by and consistent with law, University policy, or campus policy; (ii) when formally requested by an authorized office of the University as part of an official security investigation; (iii) when failure to act might result in

significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies, or significant liability to the Library, University, or members of the University community; or (iv) when there is substantiated reason to believe that violations of law or of University or Library policies have taken place or (v) to comply with a subpoena or court order only with the consent and advice of the University's Legal Counsel.

When under the circumstances described above personally identifiable information must be inspected, monitored, or disclosed, the following shall apply:

Authorization: Except in emergency circumstances, such actions must be authorized in advance and in writing by the University Librarian, or by the Director of Library Technology and Digital Strategies. The Library Cabinet will be notified of each authorization made. Authorization shall be limited to the least perusal of content and the least action necessary to resolve the situation.

Emergency Circumstances: In emergency circumstances -- circumstances in which delay might precipitate harm, loss, or liability as described in (iii) above -- the appropriate Library Cabinet member may approve the least perusal of content and the least action necessary to resolve the emergency, immediately and without prior written authorization, but appropriate authorization must then be sought without delay. All members of the Librarians' Council will be notified of the authorization.

Compliance with Law: Actions taken shall be in full compliance with the law and other applicable University and Library policies.

Compliance with a Subpoena or Court Order: Actions shall only be taken with the consent and advice of the University's Legal Counsel.

Privacy Limits

Library Records: Records pertaining to the business of the Library, whether or not created or recorded on Library equipment, are University records subject to disclosure under Georgia Code § 24-9-46 or to comply with a subpoena or court order.

Possession of University Records: Library employees are expected to comply with requests, properly vetted through University policies and procedures, for copies of records in their possession that pertain to the business of the University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on University electronic communications resources.

Unavoidable Inspection: During the performance of their duties, personnel who operate and support electronic communications resources periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of Library systems and services. On these and other occasions, systems personnel might observe personally identifiable information. Except as provided elsewhere in this Policy or by law, they

are not permitted to seek out such information where not germane to the foregoing purposes, or disclose or otherwise use what they have observed. Such unavoidable inspection of personally identifiable information is limited to the least invasive degree of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal and confidential information.

Except as provided above, systems personnel shall not intentionally search electronic records or transactional information for violations of law or policy. However, they shall report violations discovered inadvertently in the course of their duties to the Emory University Trust Line (www.finadmin.emory.edu/internalaudit/trustline.html).

Back-up Services

Operators of Library electronic systems shall provide information about back-up procedures to users of those systems upon request.

Changes to Our Privacy Policy

The Libraries may change our Privacy Policy at any time by posting revisions on the website. By accessing or using our website, you agree to be bound by all the terms and conditions of our Privacy Policy as posted on the website at the time of your access or use. If you do not agree to the terms of this Privacy Policy or any revised statement, please exit the site immediately.

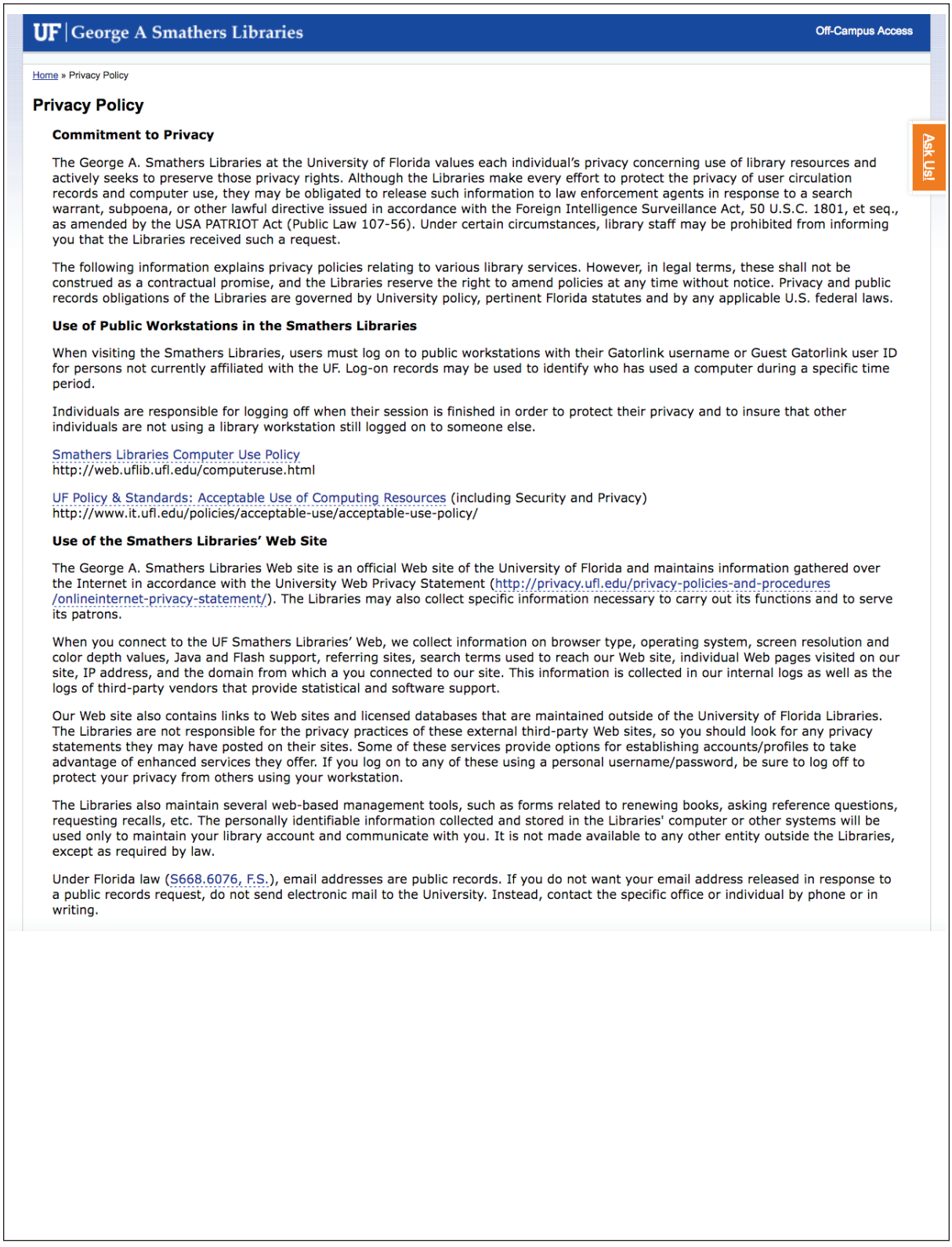
Contact Information

If you have any questions about our Privacy Policy, please contact the Administration Office of Emory University Library at 404-727-6861.

Notes

1. Personally identifiable information is any information that can be directly or indirectly associated with a known individual. For example, all information contained in personnel, patron, and circulation files is personally identifiable.
2. Library business refers to activities involved in the provision, maintenance, and management of the Library's systems and services to its patrons and staff. Circulating books and journals, enforcing Library contracts, and troubleshooting problems with the Library's e-mail system are all examples of Library business. Trying to discover who used a Library workstation to issue a harassing message would typically not be Library business, however.
3. Substantiated reason to believe requires reliable evidence, as distinguished from suspicion, rumor, gossip, or other unreliable evidence.

UNIVERSITY OF FLORIDA LIBRARIES
Privacy Policy
http://www.uflib.ufl.edu/privacy.html



UF | George A Smathers Libraries Off-Campus Access

Home » Privacy Policy

Privacy Policy

Commitment to Privacy

The George A. Smathers Libraries at the University of Florida values each individual's privacy concerning use of library resources and actively seeks to preserve those privacy rights. Although the Libraries make every effort to protect the privacy of user circulation records and computer use, they may be obligated to release such information to law enforcement agents in response to a search warrant, subpoena, or other lawful directive issued in accordance with the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801, et seq., as amended by the USA PATRIOT Act (Public Law 107-56). Under certain circumstances, library staff may be prohibited from informing you that the Libraries received such a request.

The following information explains privacy policies relating to various library services. However, in legal terms, these shall not be construed as a contractual promise, and the Libraries reserve the right to amend policies at any time without notice. Privacy and public records obligations of the Libraries are governed by University policy, pertinent Florida statutes and by any applicable U.S. federal laws.

Use of Public Workstations in the Smathers Libraries

When visiting the Smathers Libraries, users must log on to public workstations with their Gatorlink username or Guest Gatorlink user ID for persons not currently affiliated with the UF. Log-on records may be used to identify who has used a computer during a specific time period.

Individuals are responsible for logging off when their session is finished in order to protect their privacy and to insure that other individuals are not using a library workstation still logged on to someone else.

Smathers Libraries Computer Use Policy
http://web.uflib.ufl.edu/computeruse.html

UF Policy & Standards: Acceptable Use of Computing Resources (including Security and Privacy)
http://www.it.ufl.edu/policies/acceptable-use/acceptable-use-policy/

Use of the Smathers Libraries' Web Site

The George A. Smathers Libraries Web site is an official Web site of the University of Florida and maintains information gathered over the Internet in accordance with the University Web Privacy Statement (http://privacy.ufl.edu/privacy-policies-and-procedures/onlineinternet-privacy-statement/). The Libraries may also collect specific information necessary to carry out its functions and to serve its patrons.

When you connect to the UF Smathers Libraries' Web, we collect information on browser type, operating system, screen resolution and color depth values, Java and Flash support, referring sites, search terms used to reach our Web site, individual Web pages visited on our site, IP address, and the domain from which a you connected to our site. This information is collected in our internal logs as well as the logs of third-party vendors that provide statistical and software support.

Our Web site also contains links to Web sites and licensed databases that are maintained outside of the University of Florida Libraries. The Libraries are not responsible for the privacy practices of these external third-party Web sites, so you should look for any privacy statements they may have posted on their sites. Some of these services provide options for establishing accounts/profiles to take advantage of enhanced services they offer. If you log on to any of these using a personal username/password, be sure to log off to protect your privacy from others using your workstation.

The Libraries also maintain several web-based management tools, such as forms related to renewing books, asking reference questions, requesting recalls, etc. The personally identifiable information collected and stored in the Libraries' computer or other systems will be used only to maintain your library account and communicate with you. It is not made available to any other entity outside the Libraries, except as required by law.

Under Florida law (S668.6076, F.S.), email addresses are public records. If you do not want your email address released in response to a public records request, do not send electronic mail to the University. Instead, contact the specific office or individual by phone or in writing.

Ask Us!

In order to protect your privacy in regard to these services, you should always close your Web browser upon completion of your session.

Borrowing UF Libraries' Materials

The Libraries maintain personally identifiable information for library accounts of valid library users. Items charged out are, of course, linked to the individual who currently has them. Upon return of an item to the library, no record that the item has been borrowed by the individual is retained unless the item was returned overdue and resulted in an overdue fine. Records of non-returned or lost items billed to an individual for replacement are also retained for the same administrative and auditing purposes.

Library circulation records are confidential information. Library staff will not give out the name of a person who currently has an item to another library user, and will not release this information to any other entity outside the Libraries, except as required by law. (See "Confidentiality of Circulation Records" below).

Other Library Services

Confidentiality extends to information sought or received, materials consulted, database search records, reference interviews, interlibrary loan records, and other personally identifiable uses of library materials, facilities, or services. As mentioned above, any personally identifiable information collected and stored in the Libraries' computer or other systems will be used only to maintain your library account and communicate with you. It is not made available to any other entity outside the Libraries, except as required by law.

Confidentiality of Circulation Records – Florida Statutes Section 257.261

Circulation records are confidential in accordance with Section 257.261 of the Florida Statutes. The Statutes state:
"All registration and circulation records of every public library, except statistical reports of registration and circulation, are confidential and exempt from the provisions of s. 119.07(1) and from s. 24(a) of Art. I of the State Constitution. Except in accordance with proper judicial order, a person may not make known in any manner any information contained in such records, except as provided in this section. As used in this section, the term "registration records" includes any information that a library requires a patron to provide in order to become eligible to borrow books and other materials, and the term "circulation records" includes all information that identifies the patrons who borrow particular books and other materials. This section does not prohibit any library, or any business operating jointly with the library, from disclosing information to municipal or county law enforcement officials, or to judicial officials, for the purpose of recovering overdue books, documents, films, or other items or materials owned or otherwise belonging to the library. In the case of a public library patron under the age of 16, a public library may only release confidential information relating to the parent or guardian of the person under 16. Any person who violates this section is guilty of a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083."

Staff web | Departments | Conduct in the library | Contact us | Privacy policy | ADA/Accessibility | Employment | Site index

Send suggestions and comments to the library web manager.
© 2004 - 2016 University of Florida George A. Smathers Libraries.
All rights reserved.
Terms of Use for Electronic Resources and Copyright Information
This page uses Google Analytics - (Google Privacy Policy)

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

GEORGETOWN UNIVERSITY LIBRARY
Statement on Data Use for Library Assessment Purposes
https://docs.google.com/document/d/14iUMpFZFLPaLdAdpQGC9M9UgnjdkI2UBYRKGhwt9KXE/edit?usp=sharing

Statement on Data Use for Library Assessment Purposes
Submitted for approval from the Assessment Steering Committee - November 2016

The Georgetown University Library occasionally gathers data generated by library users for the following purposes:

- Respond to questions, requests, complaints, or other types of user feedback
- Provide individually customized services like faculty office delivery, InterLibrary Loan, or research consultations
- Monitor library use and demand for services
- Support technology use and network security
- Circulate books, equipment, and other library resources
- Request feedback to assess library programs or services

Data can often be helpful for communication and marketing efforts. Direct quotations from library users should only be used when consent has been given by a specific respondent, or when prior notice has been given to anonymous respondents.

The Library is committed to maintaining all data confidentially (see Confidentiality of Patron Information) and follows UIS guidelines for data security. Data gathered during an assessment project should, by default, be considered confidential, meaning that the fewest people necessary will have access to the data, including the project team, relevant department head(s), and relevant AUL(s).

During any activity that gathers feedback from users (survey, focus group, etc.) it is possible that the specific performance or behavior of an individual staff member may be referenced by a user, even if the purpose of the assessment is not to assess the staff member's performance. Sensitive data may be modified or redacted before the data set is shared widely, but an original copy of the data set will be maintained, and modified data entries will be noted within the modified data set.

Non-sensitive data sets may be anonymized and stored in a location that is accessible to all library staff members, such as the Staff Wiki or the Data Dashboard. Aggregated data sets and assessment project reports may also be shared with other Georgetown University departments when requested. To ensure workplace continuity and responsible data use, the Chair of the Assessment Steering Committee and the Assessment Librarian will have access to all data sets gathered for assessment purposes via the Library Assessment Box account.

Indiana University Libraries Privacy Policy

LIB-01

About This Policy

Effective Dates:
12-22-2003

Last Updated:
02-01-2012

Responsible University Administrator:
Dean of Indiana University Libraries

Policy Contact:
Carolyn Walters, Executive Assoc. Dean
Indiana University Libraries
cwalters@indiana.edu

Scope

All users of Indiana University Libraries.

Policy Statement

I. Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. The Indiana University (IU) Libraries define the right to privacy as the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.

The courts have recognized a right of privacy based on the Bill of Rights of the U.S. Constitution. The state of Indiana guarantees privacy in its constitution and statutory law. (See https://iga.in.gov/legislative/laws/2015/ic/titles/005/articles/014/chapters/003/ or http://www.ilfonline.org/units/confidentiality/). IU Libraries' privacy and confidentiality policies are intended to comply with applicable federal, state, and local laws, as well as with any IU policies on privacy, including the Indiana University policy on Privacy of Electronic Information and Information Technology Resources; a set of frequently asked questions to accompany this policy can be found at: http://protect.iu.edu/cybersecurity/policies/IT07/faq. In addition, this privacy policy conforms to the requirements of the IU policy on Web Site Privacy Notices.

User rights--as well as our institution's responsibilities--outlined here are based in part on what are known in the United States as the five "Fair Information Practice Principles." These five principles outline the rights of Notice, Choice, Access, Security, and Enforcement.

Our commitment to our users' privacy and confidentiality has deep roots not only in law but also in the ethics and practices of librarianship. In accordance with the American Library Association's Code of Ethics:

"We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted." (http://www.ala.org/advocacy/proethics/codeofethics/codeethics)

II. Applicability

This privacy notice applies only to the Indiana University (IU) Libraries and explains our practices concerning the collection, use, and disclosure of user information. Users' information collected by the Indiana University Libraries will be used only as outlined in this privacy notice.

Other units at the University may collect and use visitor information in different ways. Therefore, visitors to other University web sites and those who interact with University units and departments should review the privacy notices for those units or for the particular University web sites they visit. The IU Libraries are not responsible for the content of other web sites or for the privacy practices of University units or web sites outside the scope of this notice.

III. Indiana University Libraries' Commitment to Our Users' Rights of Privacy and Confidentiality

This privacy policy explains our users' privacy and confidentiality rights, the steps the IU Libraries take to respect and protect privacy, and how we deal with personally identifiable information that we may collect from our users.

1. Notice & Openness

The IU Libraries affirm that our library users have the right of "notice" -- to be informed about the policies governing the amount and retention of personally identifiable information, and about why that information is necessary for the provision of library services.
The IU Libraries post publicly and acknowledge openly the privacy and information-gathering policies of the IU Libraries. Whenever policies change, notice of those changes is made publicly available. In all cases involving personally identifiable information, it is our policy to avoid creating unnecessary records; to avoid retaining records not needed for the fulfillment of the mission of the library; and to avoid engaging in practices that might place sensitive information on public view.
Information that the IU Libraries may gather and retain about current and valid library users includes, but is not limited to, the following:

Circulation Information
This includes all information that identifies a user as borrowing specific materials, including reserve materials.
Collection Development and Resource Management
This includes information regarding the request, purchase, transfer, and related collection management requests linked to individual users or groups of users (e.g., departments).
Electronic Access Information
This includes all information that identifies a user as accessing specific electronic resources, whether library subscription resources, electronic reserves, or other Web resources.
Interlibrary Loan/Document Delivery
This includes all information that identifies a user as requesting specific materials.
Library Surveys/Assessment Projects
This includes any information or data obtained by any IU library through surveys (group or individual interviews or other means) in support of assessment of services, collections, facilities, resources, etc., or in support of research related to library and information services. Any data collected in the course of research is subject to additional review of privacy and confidentiality protections.
Reference/Research Consultations
This includes any information regarding the identity of library users, the nature of their inquiry, and the resources that they consult.
User Registration Information
This includes any information the library requires users (faculty, staff, students, or others) to provide in order to become eligible to access or borrow materials. Such information includes addresses, telephone numbers, and identification numbers.
Other Information Required to Provide Library Services
This includes any identifying information obtained to provide library services not previously listed.

2. Choice & Consent

This policy explains our information practices and the choices users can make about the way the IU Libraries collect and use this information.
To provide borrowing privileges, we must obtain certain information about our users in order to provide them with a library account. If users are affiliated with Indiana University, the library automatically receives personally identifiable information (name, address, e-mail address, status [as student, faculty, staff], identification number, etc.) in order to create and update their library account from the Registrar's Office (for students) or Human Resources (for employees). When visiting our library's web site and using our electronic services, users may choose to provide their name, e-mail address, library card barcode, phone number or home address.
Users who are not affiliated with Indiana University have the option of providing us with their e-mail address for the purpose of notifying them about their library account. Users may request that we remove their email address from their record at any time.
The IU Libraries never use or share the personally identifiable information provided to us in ways unrelated to the ones described above without also providing users an opportunity to prohibit such unrelated uses, unless we are compelled to do so under the law. Our goal is to collect and retain only the information we need to provide library-related services. The IU Libraries strive to keep all personally identifiable information confidential and do not sell, license, or disclose personal information without consent unless compelled to do so under the law or as necessary to protect library resources or conduct necessary library operations.

3. Access by Users

We attempt to fulfill all requests made by individuals who use library services that require the provision of personally identifiable information and to update their information through proper channels. Users may be asked to provide some sort of verification (e.g., PIN number, photo or network identification card, etc.) to ensure verification of identity.

4. Data Integrity & Security

The data we collect and maintain at the library must be accurate and secure. Although no method can guarantee the complete security of data, we take steps to protect the privacy and accuracy of user data in the following ways:

> *Data Integrity:* We take reasonable steps to assure data integrity, including: using only reputable sources of data; providing our users access to their own personally identifiable data; updating data whenever possible; utilizing middleware authentication systems that authorize use without requiring personally identifiable information; destroying untimely data or converting it to anonymous form.
> *Data Retention:* We regularly review and purge personally identifiable information once it is no longer needed to manage library services. Information that is regularly reviewed for purging includes, but is not limited to, personally identifiable information on library resource use, material circulation history, and security/surveillance tapes and logs.

The IU Libraries are committed to investing in appropriate technology to protect the security of personally identifiable information while it is in the library's custody. The IU Libraries follow University policy for the retention of data, and access to data is restricted to a small number of authorized university computing personnel. The IU Libraries post announcements about the choice users make in signing up for customized or personalized services related to web and database services.

> *Services that Require User Login:* In-library computers allow guest use of most library resources without logging in. Use of the full resources of the World Wide Web and of the full power of some subscription databases requires that a user log on to the workstation, either with his/her network ID and password or with a special guest account the user obtains from the library. Data about which users were connected to which machine is collected, in accordance with University policy, and kept for a limited time with very limited access by staff. Users of electronic resources that require authorization for their use are also asked to log in when they connect from outside the university IP address ranges. The data kept from these transactions does not include information linking the user to the resources to which the user connected or about searches completed and records viewed.
> *Cookies:* Cookies are used by IUCAT to maintain the persistence of a default library search limit. These cookies are session cookies and are removed when the user exits the catalog and closes the browser.

Some licensed databases also use cookies to remember information and provide services while the user is online. Users must have cookies enabled to use these resources.

IU Libraries' web sites provide links to other, non-university sites. Indiana University is not responsible for the availability, content, or privacy practices of those sites. Non-university web sites are not bound by this privacy policy and may or may not have their own privacy policies. We are, however, committed to working with vendors of library resources to find solutions that respect the user's privacy and we include a review of the privacy policy espoused by the vendor in purchasing decisions. We provide users with information about the risks of providing personally identifiable information so that they can make reasonable choices about use of personalized services from vendors of electronic library materials. We discourage users from choosing passwords or PINs that could reveal their identity, including Social Security numbers. We regularly remove cookies, web history, cached files, and other use records from library computers and networks.

Security Measures: Our security measures involve both managerial and technical policies and procedures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Our managerial measures include internal organizational procedures that limit access to data and prohibit those individuals with access from utilizing the data for unauthorized purposes. Our technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and storage of data on secure servers or computers that are inaccessible from a modem or network connection.
Staff access to personal data: We permit only authorized Library staff with assigned confidential passwords to access personal data stored in the Library's computer system for the purpose of performing library work. The IU Libraries will not disclose any personal data collected from users to any other party except where required by law, to report a suspected violation of law or University policy, or to fulfill an individual user's service request. We do not sell or lease users' personal information to commercial enterprises, organizations or individuals.

5. Children

This site is not directed to children under 13 years of age, does not sell products or services intended for purchase by children, and does not knowingly collect or store any personal information, even in aggregate, about children under the age of 13. We encourage parents and teachers to be involved in children's Internet explorations. It is particularly important for parents to guide their children when they are asked to provide personal information online.

6. Use of Third Party Analytics Software

Web site developers and owners review usage data on their web pages to identify resources that are being used and to evaluate the provision of information on the site and the effectiveness of the organization and design of that information. This usage data is provided by traditional packaged software and by third-party services. The IU Libraries only use third party analytics software from reputable organizations that have strong privacy policies. Web sites provided by the IU Libraries may use Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to help the website analyze how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser; however please note that if you do this you may not be able to use the full functionality of IU Libraries websites and linked electronic resources.
IU Libraries that use data from Google Analytics and other third-party software providers use such data in the aggregate and do not associate use of any web page or any resource with a particular computer or a particular user.
By using IU Libraries' websites, you consent to the processing of data about you by Google and other providers of usage data in the manner and for the purposes set out above.

7. Enforcement & Redress

The IU Libraries will not make library records available to any agency of state, federal, or local government unless required to do so under law or to report a suspected violation of the law. Nor will we share data on individuals with other parties including faculty, staff (including library staff except in the performance of their assigned duties), parents, students, campus security, and law enforcement personnel, except as required by law or University policy or as needed to perform our University duties.
Library staff are to refer all requests for confidential user records to the appropriate Library Dean or Director or their designate. Only the Library Dean/Director or designate has authorization to receive and respond to requests from law enforcement or other third parties. The Dean/Director will forward all requests from law enforcement or other government officials, all requests under applicable "open records" laws, to University Counsel, and will consult with counsel regarding the proper response. Each library within Indiana University will develop written procedures to comply with this policy.
We conduct regular privacy audits in order to ensure that all library programs and services are enforcing our privacy policy. Library users who have questions, concerns, or complaints about the library's handing of their personally identifiable data should file written comments with the director of the library in question. We will respond in a timely manner and may conduct a privacy investigation or review our policy and procedures.
If you feel that the IU Libraries are not following this stated policy and communicating with the Libraries does not resolve the matter, or if you have general questions or concerns about privacy at Indiana University, please contact the University Chief Privacy Officer, 812-855-8476 or privacy@iu.edu.

History

This policy went into effect on December 22, 2003 and was last revised on February 1, 2012.

The latest revision was approved by University Counsel (2/13/2012) and the Council of Head Librarians (2/17/2012).

Related Information

IT-07, Privacy of Electronic Information and Information Technology Resources
IT-07, FAQ
ISPP-24, Web Site Privacy Notices
Indiana Code 5-14-3, Access to Public Records
Indiana Library Federation, Confidentiality of Library Records State of Indiana

UNIVERSITY OF MARYLAND

Today: **McKeldin** 08:00AM - 10:00PM

Home / **About** / Privacy Information

Privacy Information

Introduction

The UMD Libraries respects the privacy of library users in accordance with the American Library Association's document ***Privacy: An Interpretation of the Library Bill of Rights***

"*Users have the right to be informed what policies and procedures govern the amount and retention of personally identifiable information, why that information is necessary for the library, and what the user can do to maintain his or her privacy.*"

Although the University of Maryland Libraries make every effort to protect the privacy of user circulation records (including books and Internet searches), the Libraries and the Division of Information Technology (DIT) with respect to the use of public Libraries work stations may be obligated to release such information to law enforcement agents in response to a search warrant or subpoena, such as those issued in accordance with the Foreign Intelligence Surveillance Act, 50 U.S.C. 1861, as amended by the **USA PATRIOT Act (Public Law 107-56)**. That law prohibits library staff from informing you that it received such a request.

Information We Collect and How it is Used

The user information collected by the Libraries is necessary to provide the requested library services (e.g. book or article delivery), to transfer a reference query to a third party, to comply with license agreements to limit certain electronic resources to the UMD community, and to evaluate and assess our chat and email reference services. Individual server use is not made public.

The following services may require the patron to submit personal information: Aleph - online catalog; e-mail / web forms (e.g., *Ask a Librarian*) and off-campus access to restricted resources (e.g., licensed databases accessed through *Database Finder*, interlibrary loan). Three categories of personal information are collected:

- *Data that are automatically collected* due to Information Technology systems include your browser type, and the domain and Internet Protocol (IP) address from which and to which you are connecting; the source and destination network ports; the date and time of your visit to the site, and the number of bytes transmitted. URLs are not captured. OIT retains login/logout data for up to 8 weeks and Internet transaction data for up to 4 weeks.
- *Data that are collected at the user's request* to customize library services

include personalized settings, such as search preferences on the catalog or in *Database Finder*, marked items, and saved searches.

- *Data that are collected in the course of the day-to-day business* of circulating materials and providing online reference services include your UMD ID number, address, phone number, e-mail address, circulation record, and service requests (e.g., interlibrary loan and reference question).

Circulation records that the University Libraries maintain that contain personally identifiable information about an individual and his/her use of University Libraries facilities may not be inspected or disclosed under the Maryland Public Records Act except by personnel to perform typical Library business. They may be released in response to a search warrant, subpoena or other legal process.

Cookies

Cookies are small pieces of data sent by a Web server and stored by the Web browser. Cookies are used to remember information about preferences and pages visited. For example, if a user's name and password were stored as a cookie, it would save that person from entering the same information when accessing the same service subsequent times during the same browser session. Our website utilizes Google Analytics, a service which uses cookies to collect non-personally identifiable information about website usage (see the **Google Analytics privacy policy** for more information). This data is aggregated and delivered to the Libraries so that we can improve the function and content of our website. Data typically collected include browser used; web pages requested; referring web page; Network Location; screen resolution; date and time. One can refuse to accept or disable cookies by adjusting the browser's settings.

Security

UMD Libraries are committed to keeping personally identifiable information that is required to provide services for the shortest amount of time necessary to complete and manage library transactions. Access to personal information is limited to library staff who need it to provide library services.

Our website contains links to external websites and licensed databases. The University Libraries are not responsible for the privacy practices, security, or content of these external websites. We recommend that you familiarize yourself with the privacy and security information for any site you visit. While we do whatever we can to protect your privacy, please be aware that information or files transferred via the Internet or stored on Internet-accessible computers may be vulnerable to unscrupulous users. Just as in the investing world, you must protect yourself, please be careful and responsible whenever you are online.

Questions?

If you have questions or comments about the UMD Libraries privacy policies and procedures, please contact:

Public Services Division Office, McKeldin Library, Room 4119, University of

Penn State University Libraries (/) MENU

Pattee and Paterno - 7:45 am to 9:00 pm (/hours-and-locations)

Policy UL-AD08 Confidentiality and Privacy of Patron Library Records

Main Policy Content

Contents:

- Purpose
- Introduction
- University Libraries' Policies
  - Library Records
  - E-Mail and Internet
- Applicability and Guidelines
- Family Educational Rights and Privacy Act (FERPA)
- Cross References

PURPOSE:

This document codifies the policies of University Libraries regarding privacy of users' records.

INTRODUCTION:

It is the policy of the Pennsylvania State University Libraries that the privacy of all users, including employees, shall be respected in compliance with federal and state laws and professional standards of confidentiality. This policy applies to all resources regardless of their format or means of delivery as well as to all services offered by the Libraries. We maintain strict client confidentiality and will not reveal the identities of individual users or reveal what information resources they consult or services provided to them to any non-Libraries staff, individual, or entity without a court order or a valid subpoena, or under appropriate federal law.

The University Libraries comply with the American Library Association's Code of Ethics (http://www.ala.org/ala/issuesadvocacy/proethics/codeofethics/codeethics.cfm) that states:

We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.

(June 28, 1995)

We also adhere to the Pennsylvania Statute covering the confidentiality of library records that states:

Library circulation records:

Records related to the circulation of library materials which contain the names or other personally identifying details regarding the users of the State Library or any local library which is established or maintained under any law of the Commonwealth or the library of any university, college or educational institution chartered by the Commonwealth or the library of any public school or branch reading room, deposit station or agency operated in connection therewith, shall be confidential and shall not be made available to anyone except by a court order in a criminal proceeding. (24 P.S. § 9375, 2012 (http://www.legis.state.pa.us/cfdocs/legis/li/consCheck.cfm?txtType=HTM&ttl=24&div=00.&chpt=000.&sctn=000.&subsctn=000.))

Many of the University Libraries' records may also be protected under the Family Educational Rights and Privacy Act (FERPA). [See section on FERPA (https://www.libraries.psu.edu/policies/ul-ad08#ferpa)]

UNIVERSITY LIBRARIES POLICIES:

Library Records:

Records of the borrowing and use of library materials and equipment are considered to be confidential, as are the records of patron transactions of any type including, but not limited to, reference interactions, computer use logs, logs of Internet sites consulted, etc., as well as records of transactions regarding fees and fines. For library purposes, this covers all records related to the circulation or use of laptop computers, camcorders, digital cameras, and any other equipment loaned by the University Libraries as well as books, periodicals, and other formats of printed or electronic information available from the Libraries, including materials that are personally owned by a faculty member that have been placed on reserve for reading in a course. Reference or other service transactions, whether conducted in person, in writing, by telephone, via electronic mail or online interaction, are also considered confidential. Information will be disclosed to law enforcement officials upon request by court order or valid subpoena, or in compliance with appropriate federal law without prior notice.

E-mail and Internet:

E-mail and Internet connections are provided to assist and facilitate library communications. All user files and logs of user transactions on the University and Libraries' systems are held to be confidential and will be kept as private as possible. Collection and analysis of data on usage of the licensed commercial online databases and materials offered by the Libraries through its system assists both the publisher and the University Libraries to understand the impact of this technology and service. We request that any such usage data compiled by the licensor will be collected by a method consistent with applicable privacy laws and written confidentiality requirements of the licensing agreement. Any usage data available, such as number of searches or articles downloaded, is reported at least quarterly by the licensor to the University and is confidential under this policy. Information will be disclosed to law enforcement officials upon request by court order or valid subpoena or under appropriate federal law without prior notice

The University and Libraries reserve the right to inspect, view and access all data files, electronic messages, and logs of Internet sites consulted by any individuals if it is suspected that the system has been used outside of acceptable use as defined by University policy AD96 Acceptable Use of University Information Resources.

[direct quote from AD96 section II. PRINCIPLES OF ACCEPTABLE USE:]

All individuals' granted access to Penn State information technology resources must agree to and accept the following:

- Using only the information technology resources for which they are authorized by the University.
- Utilizing appropriate authentication mechanisms to access information technology resources.
- Not attempting to access information technology resources for which their authorization may be erroneous or inadvertent.
- Only using accounts, passwords, and/or authentication credentialsthat have been authorized to use consistent with their role at Penn State.
- Protecting, and not sharing, their account, password, and/or authentication credentials.
- Only sharing data with others as defined by applicable policies and procedures, and dependent on their assigned role.
- Not using Penn State information technology resources to represent the interests of any non-University group or organization unless authorized by an appropriate University department or office or that could be taken to representPenn State.
- Not using any hardware or software designed to assess or weaken security strength, unless authorized by the institutional CISO or his or her designee(s).
- Not engaging in disruptive "spamming" (i.e., sending unsolicited electronic communicationto groups of recipients at the same time), or acting in a way that will harm, damage, corrupt, or impede authorized access to information resources, systems, networks, equipment, and/or data.
- Not forging identities or sending anonymous messages, unless the recipient has agreed to receive anonymous messages.
- Not using Penn State information technology resources to alter, disrupt, or damage information technology resources of another person or entity.
- Not using Penn State information technology resources to upload, download or distribute copyrighted or illegal material which results in violation of law.
- Complying with all licenses and contracts related to information technology systems which are owned, leased, or subscribed to by Penn State, and complying with applicable local, state or federal laws, and institutional policies, rules, and guidelines as they relate to information technology resources.

In the event of suspected misuse of Libraries' computational services, the Libraries will act in accordance with the University's Office of Information Security, and in accordance with University policies AD96 Acceptable Use of University Information Resources (https://policies.psu.edu/policies/ad96) and AD95 – (https://policies.psu.edu/policies/ad95)Information and Assurance and IT Security (https://policies.psu.edu/policies/ad95) (Formerly AD20 Computer and Network Security).

APPLICABILITY AND GUIDELINES:

Any request for patron information that library staff may receive from a law enforcement official should be referred directly to the Dean's office, 510 Paterno Library, University Park, (814) 863-4723.

All Libraries staff and faculty must follow the procedures contained in the Staff Guidelines on Protecting the Confidentiality and Privacy of Patron Library Records [UL-ADG04 (https://www.libraries.psu.edu/policies/ul-adg04)]. This applies to all requests for information regarding our library users as well as an individual's library records, etc. This applies to all University Library locations and offices during all hours of service.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA):

The Family Educational Rights and Privacy Act (also known as FERPA) protects the privacy of students' educational records, including student library financial records. Pursuant to University Policy AD11 (http://guru.psu.edu/policies/AD11.html) on Confidentiality of Student Records, the University Libraries ensure compliance with FERPA by not disclosing information about a student's record to any third party, including parents, personnel in an academic department, or other individuals.

Unless there is prior written approval allowing disclosure, the parent (or third party) should be referred back to the account holder (the student) for an explanation. The most frequent inquiry made by parents is about students' library fees that appear on their Bursar Account Statements.

Libraries personnel will annotate the note field in the student's circulation record with a reference to the form on file and refer inquiries to the Libraries' Business Office. Forms will be maintained for no more than three years after the student signature has been affixed.

When there is no form on file, inquiries must be referred back to the student.

CROSS REFERENCES:

Guideline UL-ADG04 (https://www.libraries.psu.edu/policies/ul-adg04) Staff Guidelines on Protecting the Confidentiality and Privacy of Patron Library Records

Effective Date: October 3, 2003
Date Approved: October 3, 2003 (Dean's Library Council; University Legal Counsel)

Revision History (and effective dates):

- December 2017 – Revised to make the E-mail and Internet section current
- August 31, 2015 – Editorial revisions
- March 17, 2008 – Addition of section on FERPA
- October 3, 2003 – Supersedes January 2002 policy
- January 14, 2002 – New policy

Last Review Date: September 2010

Syracuse University
Libraries

PRIVACY POLICY

Introduction

The Syracuse University Libraries ("Libraries") are committed to protecting the privacy of all who use their services, in person or online. This Privacy Policy provides information about the information the Libraries collect and use, and why they use such information.

The Libraries provide a vast array of services. Many services do not require users to divulge any information to Libraries staff or systems. Other services, however, require users to provide some information in order to receive or benefit from the service.

At all times, the Libraries' staff keeps confidential all information about our users, their activities, and their research choices to the extent allowed by law. All Libraries divisions and personnel comply with New York State law that governs the confidentiality of library records.

The remainder of this Privacy Policy provides details about the Libraries' collection and use of various types of information. If you have any questions, comments, or concerns about this policy, please contact the Director of the Copyright & Information Policy Office at cipa@syr.edu.

Definitions

"Individual Information" includes personal name, physical addresses (including permanent and temporary residence addresses), electronic addresses (including e-mail, instant messaging addresses or screen names, and VOIP addresses or screen names), telephone numbers, and social security number.

"University Information" includes SU ID number, NetID, and any cards or items that include such numbers or identifiers.

"Authenticated Services" are Web-based services the Libraries provide through the Libraries website that require proof that the visitor using the service is affiliated with the Syracuse University community. Authenticated Services - such as "Request," "My Account," "My Bookbag," and using databases off campus - may require users to provide University information.

The **"Libraries Website"** includes content, files, and servers the Libraries manage or control, including, but not limited to, those under the addresses http://library.syr.edu; http://summit.syr.edu; http://syracuse.summon.serialssolutions.com/; http://copyright.syr.edu; and associated or successor websites or portals that manage, display or provide information about the Libraries' collections or holdings.

Libraries Privacy Policy (Version 2.0)
Updated October 4, 2013

"Business Transactions" are agreements between individuals or institutions and the Libraries that may have federal or state income tax, trust, or estate implications.

New York State Law

New York State law (N.Y. C.P.L.R. § 4509), which outlines the confidentiality of patron records, says in substantive part:

> Library records, which contain names or other personally identifying details regarding the users of ... college and university ... shall be confidential and shall not be disclosed except that such records may be disclosed to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute.

"**Library records**" include information related to:

- circulation of library materials;
- computer database searches;
- interlibrary loan transactions;
- reference queries;
- requests for photocopies of library materials;
- title reserve requests; or
- the use of audio-visual materials, films or records.

The Libraries and their staff comply with New York's law concerning the confidentiality of patron records.

Details on Libraries' Information Gathering

The Libraries perform many functions for the University community. This section provides details about the Libraries' information gathering practices with respect to each service the Libraries provide to patrons.

1. **Browsing the Libraries website:** The Libraries collect and store certain information automatically when people browse the Libraries' website. This information includes:

    - Internet domain (e.g., .edu for educational accounts, .com for commercial accounts);
    - IP address;
    - type of browser and operating system used;
    - date and time of access;
    - pages visited; and
    - referring URL.

The Libraries use this information to track site usage, monitor site performance, and generate aggregate statistics. The Libraries, however, do not record, maintain, or track any Individual Information or University Information while visitors are browsing portions of the Libraries website that do not contain Authenticated Services.

2. **Reference**: When visitors seek assistance at the reference desk, the Libraries do not require them to provide Individual Information or University Information. The Libraries may require a visitor to provide University Information, however, in order to use the Libraries' online resources. Also, the Libraries may ask users for Individual Information or University Information in order to improve or customize online or face-to-face reference services.

   The Libraries may use information they collect during reference transactions for internal business purposes and to improve the Libraries' services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.
3. **Classic Catalog:** When users browse or search the Classic Catalog, the Libraries' online public access catalog, the Libraries collect and store information that is similar to what they collect when visitors browse the Libraries website. If visitors seek to use Authenticated Services within the Classic Catalog, however, they must provide University Information.

   The Libraries may use information they collect from the Classic Catalog system for internal business purposes and to improve Libraries services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.
4. **Circulation:** The Libraries require all users to provide University Information in order to borrow materials from the Libraries, including books and laptop computers.

   The Libraries may use circulation information they collect for internal business purposes and to improve Libraries services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.
5. **Interlibrary Loan:** The Libraries require all users to provide University Information in order to borrow materials from other libraries through the inter-library loan ("ILL") service.

   The Libraries may use ILL information they collect for internal business purposes and to improve the Libraries' services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.

Libraries Privacy Policy (Version 2.0)
Updated October 4, 2013

6. **Online Resources**: When a member of the University community is on campus, that person can access the Libraries' online resources without having to provide Individual Information or University Information. (This presumes a person already has logged on to the University network, which requires providing University Information.)

   When a member of the University community is off campus, however, that person will be required to provide University Information in order to use the Libraries' online databases.

   The Libraries may use information that they collect about online database use for internal business purposes and to improve the Libraries services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.
7. **Technology Loan:** The Libraries require all users to provide University Information in order to borrow technology items.
   The Libraries may use University Information and associated data loan information if users fail to return the items as required by the Libraries Technology Support & Loan Policy. Whenever this occurs, the Libraries will provide University Information to the Syracuse University Bursar or the Syracuse University Department of Public Safety. The Libraries will also enable tracking software installed on the technology items to identify their location; tracking may include the use of cameras.
8. **Libraries Research Initiatives**: In order to improve their service to the community, the Libraries occasionally may conduct survey studies, issue questionnaires, or perform other data gathering activities. During these initiatives, the Libraries may ask visitors to provide Individual Information or University Information. In these circumstances, the Libraries consider this information optional; the visitor or user can choose whether or not to provide this information. Further, a visitor's decision to withhold Individual Information or University Information from a Libraries employee who is conducting a research initiative will not harm, diminish, or otherwise affect the level of service that visitor receives from the Libraries.

   The Libraries may use information that they collect from research initiatives for internal business purposes and to improve the Libraries' services. Whenever this occurs, the Libraries will use the information in a way that eliminates all Individual Information, and strips any personally identifying connectors from University Information.

9. **Business Transactions:** Under federal or state law, the Libraries may be required to collect, track, and keep Individual Information whenever they conduct a Business Transaction with an individual or institution. In these cases, Individual Information may include taxpayer identification numbers.

The Libraries may use information that they collect from Business Transactions for internal business purposes only. Whenever this occurs, the Libraries will divulge Individual Information only to the following parties:

- University officials who are authorized to handle such information;
- state or federal taxing agencies upon official, written request;
- an individual's duly authorized attorney or estate executor; and/or
- an organization's duly authorized representative, upon written request.

The Libraries retain Individual Information associated with Business Transactions for a period of time mandated by state or federal tax laws, and consistent with the University's data retention schedule.

Summary

This chart summarizes the Libraries' information gathering practices.

Service	Service Type	Individual Information Required?	University Information Required?
Web site browsing	Browsing only	No	No
Web site browsing	Authenticated services[1]	No	Yes
Reference[2]	In-Person	No	No
Reference[2]	Online	Optional	Yes
Catalog (SUMMIT)	Browsing only	No	No
Catalog (SUMMIT)	Authenticated services[1]	No	Yes
Circulation	All	No	Yes
Inter-Library Loan	All	Yes	Yes
Online Databases[3]	On-campus	No	Maybe
Online Databases[3]	Off-campus	No	Yes
Technology Loan	All	Yes	Yes
Library Research Initiatives	All	Optional	Optional
Business transactions[4]	All	Yes	No

Notes:

[1]Authenticated services often require University Identification. Includes consultations with the Copyright & Information Policy Adviser.

[2]On-campus, wireless use of online databases presumes prior authentication to the University network (including AirOrange).

[3]University Information is required to login from a Library computer workstation.

[4]Federal regulations may require taxpayer identification numbers for certain Business Transactions (including selling books to the Library).

Libraries Privacy Policy (Version 2.0)
Updated October 4, 2013

Social Security Numbers

There is no service the Libraries provide - in person or online - that requires a user to provide his or her social security number. Except for Business Transactions, if a Libraries staff member or affiliated Libraries service (including an online database) requests your social security number, please contact the Director of the Libraries' Copyright & Information Policy Office immediately at cipa@syr.edu.

Personal Security

Users share in the responsibility for ensuring that their personal information is adequately protected. It is users' responsibility to protect their University Information. When using the Libraries' computers, users must keep their University Information secure from unauthorized access by keeping their password secret. Users must never leave the Libraries' computers unattended while logged in using University Information. Users must always log out of the Libraries' computers if stepping away from the Libraries' computers.

Links to Other Websites

The Libraries' websites may contain links to other websites of interest. Once users visit such other sites, the Libraries cannot control the protection and privacy of any information users provide on those other sites. Users should exercise caution and look at the privacy statement applicable to the website in question.

Contact

If you have any questions about this Privacy Policy, please contact us through our website or write to the Libraries at:

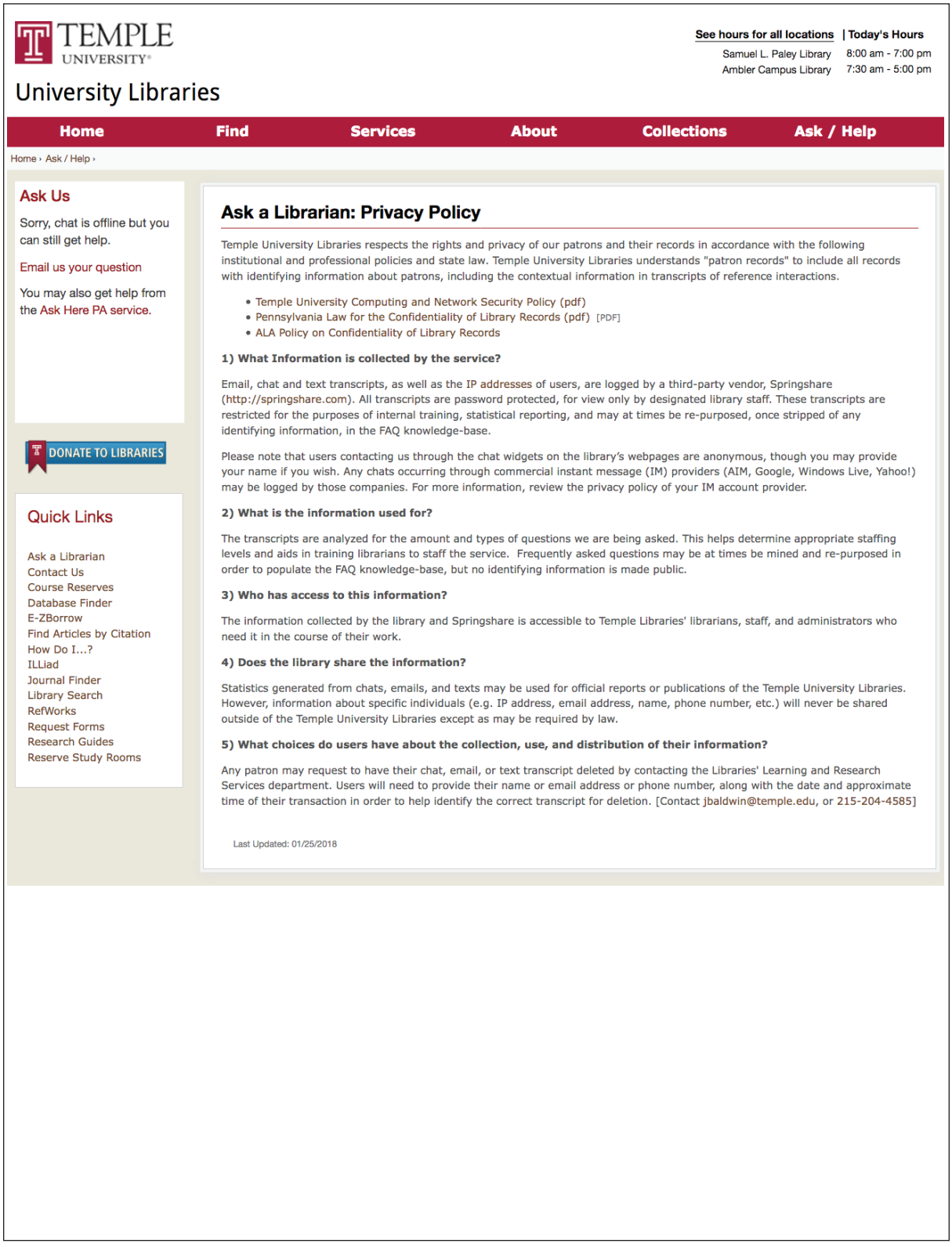
Syracuse University Libraries
222 Waverly Avenue
Syracuse, New York 13244
Attn: Director, Copyright & Information Policy Office
E-mail: cipa@syr.edu

Metadata

Version: 2.0
Author: Pamela W. McLaughlin
Editors: K. Matthew Dames; Amy Vanderlyke Dygert
Date: August 1, 2009; October4, 2013
URL: http://library.syr.edu/policies/privacy.html
Contact: cipa@syr.edu

Libraries Privacy Policy (Version 2.0)
Updated October 4, 2013

TEMPLE UNIVERSITY LIBRARIES
Ask a Librarian: Privacy Policy
https://library.temple.edu/asktulibraries/privacy



TEMPLE UNIVERSITY
University Libraries

See hours for all locations | Today's Hours
Samuel L. Paley Library 8:00 am - 7:00 pm
Ambler Campus Library 7:30 am - 5:00 pm

Home | Find | Services | About | Collections | Ask / Help

Home › Ask / Help ›

Ask Us

Sorry, chat is offline but you can still get help.

Email us your question

You may also get help from the Ask Here PA service.

DONATE TO LIBRARIES

Quick Links

Ask a Librarian
Contact Us
Course Reserves
Database Finder
E-ZBorrow
Find Articles by Citation
How Do I...?
ILLiad
Journal Finder
Library Search
RefWorks
Request Forms
Research Guides
Reserve Study Rooms

Ask a Librarian: Privacy Policy

Temple University Libraries respects the rights and privacy of our patrons and their records in accordance with the following institutional and professional policies and state law. Temple University Libraries understands "patron records" to include all records with identifying information about patrons, including the contextual information in transcripts of reference interactions.

- Temple University Computing and Network Security Policy (pdf)
- Pennsylvania Law for the Confidentiality of Library Records (pdf) [PDF]
- ALA Policy on Confidentiality of Library Records

1) What Information is collected by the service?

Email, chat and text transcripts, as well as the IP addresses of users, are logged by a third-party vendor, Springshare (http://springshare.com). All transcripts are password protected, for view only by designated library staff. These transcripts are restricted for the purposes of internal training, statistical reporting, and may at times be re-purposed, once stripped of any identifying information, in the FAQ knowledge-base.

Please note that users contacting us through the chat widgets on the library's webpages are anonymous, though you may provide your name if you wish. Any chats occurring through commercial instant message (IM) providers (AIM, Google, Windows Live, Yahoo!) may be logged by those companies. For more information, review the privacy policy of your IM account provider.

2) What is the information used for?

The transcripts are analyzed for the amount and types of questions we are being asked. This helps determine appropriate staffing levels and aids in training librarians to staff the service. Frequently asked questions may be at times be mined and re-purposed in order to populate the FAQ knowledge-base, but no identifying information is made public.

3) Who has access to this information?

The information collected by the library and Springshare is accessible to Temple Libraries' librarians, staff, and administrators who need it in the course of their work.

4) Does the library share the information?

Statistics generated from chats, emails, and texts may be used for official reports or publications of the Temple University Libraries. However, information about specific individuals (e.g. IP address, email address, name, phone number, etc.) will never be shared outside of the Temple University Libraries except as may be required by law.

5) What choices do users have about the collection, use, and distribution of their information?

Any patron may request to have their chat, email, or text transcript deleted by contacting the Libraries' Learning and Research Services department. Users will need to provide their name or email address or phone number, along with the date and approximate time of their transaction in order to help identify the correct transcript for deletion. [Contact jbaldwin@temple.edu, or 215-204-4585]

Last Updated: 01/25/2018



University Libraries

WU Libraries Privacy Statement

Thank you for visiting the Washington University Libraries website and reviewing our privacy policy. Our privacy policy is clear: We will collect no personal information about you when you visit our website unless you choose to provide that information to us, such as by submitting a question, requesting an item, or otherwise 'doing business' with the Libraries.

> *Although we try to protect the privacy of user records (including books and Internet searches), the Libraries may be obligated to release such information to law enforcement agents in accordance with state or federal law. Unless otherwise precluded by law, the Libraries will inform library users that their records have been accessed. Please see Confidentiality of Washington University Library Records for more information.*

The following discloses the information gathering and dissemination practices of the University Libraries for these websites:*library.wustl.edu*, *catalog.wustl.edu (spokane.wustl.edu)*, *libcat.wustl.edu*, *illiad.wustl.edu*, *ares.wustl.edu*, *orb.wulib.wustl.edu*,*digital.wustl.edu*, and any other servers running publicly-accessible library services.

INFORMATION COLLECTED AND STORED AUTOMATICALLY

If you do nothing during your visit but browse through the website, read pages, or download information, we

will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store the information usually logged by webservers: such as Internet domain and IP address; type of browser and operating system used to access our site; date and time you access our site; pages you visit; and if you linked to our website from another website, the address of that website.

We are also implementing Google Analytics to help analyze how users use the site. The tool uses "cookies," which are text files placed on your computer, to collect standard Internet log information and visitor behavior information in an anonymous form. The information generated by the cookie about your use of the website (including your IP address) is transmitted to Google. This information is then used to evaluate visitors' use of the website and to compile statistical reports on website activity for Washington University Libraries.

We will never (and will not allow any third party to) use the statistical analytics tool to track or to collect any personally identifiable information of visitors to our site. Google will not associate your IP address with any other data held by Google. Neither we nor Google will link, or seek to link, an IP address with the identity of a computer user. We will not associate any data gathered from this site with any personally identifiable information from any source, unless you explicitly submit that information (see below).

We use this information to help us make our site more useful to our primary users, the current students, faculty, and staff of Washington University.

IF YOU SEND US PERSONAL INFORMATION
If you choose to provide us with personal information as

in an email to one of our online email boxes, or by filling out a form with your personal information and submitting it to us through our website, we use that information to respond to your message and to help us get you the information you have requested. We do not collect personal information from such communications for any purpose other than to respond to you. We do not collect information for commercial marketing.

DOING BUSINESS WITH THE LIBRARIES

In order for current Washington University students, faculty, and staff to 'do business' with the Libraries – that is, check out materials, and access off-campus resources via the proxy server – the Libraries maintain a patron database. Your record in this database contains your name; address; phone number; WUSTL Key username; University ID number; a designator that indicates whether you are a student, faculty, or staff member; and your email address. It also contains information as to which items you have currently checked out, and if you owe any fines. The Libraries use the information in your patron record *only* to allow you to 'do business' with us.

We also keep information about you if you use ILLiad (Interlibrary Loan), on *illiad.wustl.edu*. Your record in this database contains your name; address; phone number; University ID number; your status with the University (student, faculty, or staff); your email address; and your WUSTL key. It also contains information about the ILL requests you have made, including the status on each request. Again, the Libraries use the information in your ILLiad record *only* to allow you to 'do business' with us.

If you are an instructor using Ares (electronic reserves), you have an account that contains your name, WUSTL key, email address and sometimes your mailing address. Ares is available only on the University campus or to people with valid library accounts. Your name is shown

on Ares to those who have the password to any of your courses with materials on Ares. You have access to this information using WUSTL key and password. If you do not know your course password, contact the Olin Reserves Unit.

If you login to *Find it!* you are creating a record on *orb.wulib.wustl.edu*. This record, in terms of what authorized library staff can view, contains only your WUSTL key username. You can save citations and your favorite sets of databases, but library staff cannot view this information.

LINKS TO OTHER SITES

This site contains many links to other sites, primarily databases and electronic journals which the Libraries have licensed for the use of Washington University students, faculty, and staff. Washington University Libraries are not responsible for the privacy practices or the content of such websites. Once you link to another site (any URL that does not begin with any of the server names listed above, outside of *.wustl.edu), you are subject to the privacy policy of the new site – which may differ considerably from the Libraries policy.

SITE SECURITY

To guard against unauthorized access, maintain data accuracy, and promote the correct use of information, we have put in place physical, electronic, and managerial procedures to safeguard and secure the information we collect online.

However, while we consider these measures reasonable, no assurance can be given that they will always and in all cases prevent or protect against invalid access or improper activity, and any expectation or warranty of unassailable site security is expressly disclaimed.

Institution Privacy Policies

Policies of Colorado State University

University Policy

Policy Title: Information Collection and Personal Records Privacy	Category: Information Technology
Owner: Vice President for Information Technology	Policy ID#: 4-1018-007
Contact: Academic Computing and Networking Services Web: http://www.acns.colostate.edu Phone: 970-491-5133	Original Effective Date: 7/21/2005 Last Major Revision: 5/10/2017 Supersedes Policy ID#: 4-1018-001

PURPOSE OF THIS POLICY

Colorado State University collects personal information of a sensitive nature to facilitate and enable its business and academic functions. Unauthorized access to such information may have significant negative consequences, including exposing those associated with the university to the risk of identity theft, and adversely affecting the reputation of the University. In addition, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Colorado House Bill 03-1175 (the "non-SSN" legislation), the Family Educational Rights and Privacy Act (FERPA), the Payment Card Industry Data Security Standard, and other legislation require various classes of information to be protected from unauthorized access. The University Policy on IT Security addresses security measures for protecting sensitive data. This policy addresses access to and use of certain sensitive information stored in paper or electronic form.

APPLICATION OF THIS POLICY

These policies encompass best practices that are in general to be applied comprehensively at the University, including third parties accessing University information. Units that own the record are responsible for implementing their aspects of this policy. All users who access sensitive digital information also must conform to this policy.

DEFINITIONS USED IN THIS POLICY

Sensitive personal information includes social security number information, personally identifiable health information, personally identifiable financial information including credit card information, personnel and student performance information, proprietary research and academic information, student and staff ID photos, and any other sensitive personal information that through disclosure may adversely affect an individual and/or the University.

Family Educational Rights and Privacy Act (FERPA): Federal law protecting students' education records from disclosure by the University to anyone other than the student without the student's consent, unless a specific exception applies.

RamCard: the official student and employee identification card issued by the University, including the official digital photo, the "RamCard ID Photo."

POLICY STATEMENT

It is Colorado State University's policy to collect and store the least amount of personally identifiable information required to fulfill its required duties and responsibilities, or to complete a particular transaction or as required by law. This policy applies to the collection and storage of all personally identifiable information, regardless of the source or medium.

For site administration functions, information (other than personal information linked to a particular individual) is collected for analysis and statistical purposes of website navigation. This information is used to help diagnose problems, assess what information is of most interest, determine technical design specifications, identify system performance or problem areas, and for other administrative functions. Such information is not subject to this policy but is covered by the IT Security Policy.

Students may choose whether or not to provide personal information to Colorado State University via the Internet. If a student chooses not to provide the personal information requested, the student may still visit most of Colorado State University's websites, but may be unable to access certain options, offers, and services.

The digital student identification picture, the RamCard ID photo, is considered personally identifiable information within the education record of the student. Student identification photos are provided digitally for use by course instructors and other CSU faculty and staff who have a legitimate educational purpose to view student

education records. These photos are not "directory information" under the FERPA policy, and may not be released to anyone without permission of the student, except in accordance with this policy. They must be secured using the same safeguards as other private and sensitive information.

Employees also have a reasonable expectation of privacy with respect to their RamCard ID photos.

POLICY PROVISIONS

1. **De Minimis Access:** The amount of sensitive personal information collected and stored shall be the minimum amount required for the efficient and effective conduct of business and academic functions. Access to sensitive personal information shall be limited to only those needing access for legitimate business or academic purposes. Periodically, individual access shall be reviewed to be in conformance with this policy.
2. Units are responsible for ensuring that all of their paper, non-paper and electronic records containing sensitive personal information are secured as required under the CSU IT Security Policy and protected from unauthorized access.
3. Periodically, units shall review their policies, operations, forms, archives and other associated functions to ensure they are in conformance with this policy.
4. Reasonable and prudent efforts shall be made to isolate and protect sensitive personal information in physical form from unauthorized access, for example in locked filing cabinets, behind locked doors, suitable IT security measures, etc.
5. Social security numbers (SSNs) shall not be used as the primary numeric identifier for individuals. This particular policy applies to all forms of information, both electronic and non-electronic, including identification cards. See the University Policy on Social Security Numbers.
6. RamCard ID Photos:
    1. Access to and use of official RamCard ID photos are permitted for legitimate educational and business purposes only. Access or use for personal reasons, and any unauthorized access or use, or redistribution, is not permitted.
    2. Direct access to the University's electronic systems that store digital ID photos must be pre-approved in writing by the Vice President for Information Technology, who shall constitute a small, ad hoc committee to review such requests. Requests must be made to the Advisory Committee for Administrative Applications (ACAdA) using the application for such access provided in Appendix A. Considerations for approval will include the business need for access,

especially inherent benefits, commitment to complying with these policy provisions, including the quality of the protections to be implemented to ensure IT security and privacy and proper data disposal, and the effort involved granting access and in implementing such protections.

3. Before access or use, departments are required to provide relevant employees a copy of this policy and ensure they understand these provisions to ensure protection of the privacy of students and employees.
4. Access and use shall be controlled via an approved login and password as specified in the CSU IT Security Policy.
5. Files containing digital ID photos shall not be copied or shared in any manner except as specifically authorized herein in advance.
6. Viewing digital photographs shall be done in a manner that is discreet, reasonably viewable only by authorized personnel.

COMPLIANCE WITH THIS POLICY

Abuse or misuse of RamCard ID photos shall be reported to the Office of the Vice President for Information Technology. Violation of this policy may result in revocation of access without notice, and may be subject to disciplinary consequences, and/or legal action.

POLICY GOVERNANCE

The Information Technology Executive Committee (ITEC) is responsible for this policy, including initiating modifications and changes as necessary to remain current with technological and legal requirements.

REFERENCES

CSU Privacy Statement and Related Information

CSU Policy on Information Technology Security

CSU Policy on Social Security Numbers

APPROVALS

Version 1.0 Approved by ITEC: July 8, 2004

Version 1.1 Approved by ITEC: July 21, 2005

Privacy of Electronic Information and Information Technology Resources

IT-07

About This Policy

Effective Dates:
01-31-2008

Last Updated:
08-17-2011

Responsible University Administrator:
Office of the Vice President for Information Technology & Chief Information Officer

Policy Contact:
University Information Policy Office, uipo@iu.edu

Scope

This policy applies to all authorized users of Indiana University information technology resources, irrespective of whether those resources or data are stored on or accessed from on-campus or off-campus locations. Unauthorized users are not protected by this policy.

Policy Statement

Stored electronic files and voice and data network communications may not be accessed by someone other than:

- the person to whom the account in which the information has been stored is assigned; or
- the person from whom the communication originated, or to whom the communication was sent; or
- the person to whom the device containing the stored electronic files has been assigned;

except in certain limited circumstances in which access is appropriate to serve or protect other core values and operations within the university as outlined in this policy. In accessing or granting access to electronic information and information technology resources, university personnel will comply with all applicable laws and university policies.

Reason For Policy

Indiana University cherishes the diversity of values and perspectives inherent in an academic institution and is therefore respectful of intellectual freedom and freedom of expression. The university does not condone censorship, nor does it endorse the routine inspection of electronic files or monitoring of network activities related to individual use. At times, however, legitimate reasons exist for persons other than the account holder to access computers, electronic files, or data related to use of the University network, including but not limited to: ensuring the continued confidentiality, integrity, and availability of university systems and operations; securing user and system data; ensuring lawful and authorized use of university systems; providing appropriately de-identified data for institutionally approved research projects; and responding to valid legal requests or demands for access to university systems and records. This policy seeks to balance individual freedom and privacy with the need for access by persons other than the account holder when necessary to serve or protect other core values and operations within the university or to meet a legal requirement.

Procedure

This policy covers:

- Data and other files, including electronic mail and voice mail, stored on, encrypted on, or in transit to or from individual computer or voice mail accounts on:
- University-owned systems/devices, or systems/devices managed by the university on behalf of affiliated organizations (e.g. Indiana University Foundation or Indiana University Alumni Association);
- University-owned computers assigned to a specific individual or group for use in support of job functions;
- University data and other university files on personally owned devices;
- Telecommunications (voice and data) traffic from, to, or between any devices described above or connected to the Indiana University technology infrastructure.

1. **Access by technicians and administrators that requires authorization**

A technician or administrator may access or permit access to specific information technology resources and electronic information as defined in this policy, in any of the following circumstances, if the technician or administrator:

1. a. **Permission Granted by Owner** - receives a written authorization from the individual to whom the account or device or communication has been assigned or attributed; or
   b. **Violations of Law or Policy** - receives a written authorization from the appropriate campus Chancellor, Provost, Human Resources Director, or Dean of Students (or equivalent) for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has engaged, is engaging, or imminently intends to engage, in illegal activities or violations of university policy using the account or device in question; or
   c. **Critical Operational Necessity** - receives a written authorization from the senior executive officer of a department for situations in which retrieving the material is critical to the operation of the department and when the account holder is deceased, terminated, incapacitated, unavailable, or unwilling to provide access; or
   d. **Deceased or Incapacitated Individual** - receives a written authorization from the senior executive officer of a department or school who has consulted with the campus Human Resources Director, Vice Provost or Vice Chancellor of Faculty & Academic Affairs (or campus equivalent), or Dean of Students to provide access to a lawful representative (e.g., spouse, parent, executor, holder of power of attorney) of a deceased or incapacitated employee, faculty member, or student; or
   e. **Internal Audit Need** - receives a directive from the Director of Internal Audit for information relating to specific audits or investigations; or
   f. **Response to Lawful Demand** - receives authorization from the Office of General Counsel confirming that access is required under the terms of a valid subpoena, warrant, other legal order, or contract, or an applicable law, regulation, or university policy; or
   g. **Substantial University Risk** – receives an authorization (written, or verbal with written confirmation) from the appropriate campus Chancellor, Provost, Vice President, or equivalent approving access after concluding that access is needed to address an emergency or to avoid or minimize exposure of the university to substantial risk of harm or liability;
   h. **Institutionally Approved Research** – receives written authorization approving access from the Institutional Review Board, any other applicable research administrative office(s), and/or the Office of General Counsel after concluding that such access is needed in support of an institutionally approved research project and the access complies with applicable laws and University policies, including rules governing the protection of human research subjects.

2. **Notification**

   A technician or administrator accessing information covered by this policy shall make reasonable efforts to report such access to the affected individual prior to that access, except:

- when prior notification is not appropriate or practical due to the urgency of the circumstances;
- when such notice may result in destruction, removal, or alteration of data; or
- when other circumstances make prior notice inappropriate or impractical.

Where prior notification is not appropriate or practical, reasonable efforts will be made to notify the affected individual as soon as possible following access unless other circumstances make follow-up notification inappropriate.

3. **Preservation of electronic information and of information technology resources**

   The copying and secure storage of the contents of an individual's email, other computer accounts, office computer, or transient network traffic to prevent destruction and loss of information may occur

   a. upon receiving credible notification of a university or law enforcement investigation for alleged illegal activity or violations of university policy on the part of a member of the university community; or
   b. upon receiving advice by the Office of General Counsel that such copying and storage is otherwise needed in order to comply with legal obligations to preserve electronic information or secure information technology resources; or
   c. upon receiving authorization from the campus Chancellor, Provost, Vice President or equivalent indicating that such preservation reasonably appears necessary to protect university operations; or
   d. when there is a reasonable belief illegal activity or violations of university policy have occurred, are occurring, or are imminently about to occur.

   Access to such copies and stored materials shall be in accordance with this policy. Preserved materials that are no longer needed must be destroyed in a secure manner.

4. **Access by technicians and administrators that does not require further authorization**

   Technicians or administrators do not require further authorization, within the scope of their legitimate university responsibilities, in any of the following circumstances:

   a. **Emergency Problem Resolution** - Technicians may access, and permit access to, information technology resources and electronic information in emergency situations, when the technician has a reasonable belief that a program or process active in the account or on the device is causing or will cause significant system or network degradation, or could cause loss/damage to a system or other users' data. This includes forensic and/or other analysis in response to a security incident, sensitive data exposure, or system/device compromise.
   b. **Collaborative Information or Resources** - Technicians may access, and permit access to, for legitimate purposes, information technology resources and electronic information that by their nature are not private, such as shared computers and shared document folders.
   c. **System-generated,**Content-neutral Information – Technicians may access and use system-generated logs and other content-neutral data describing the use of technology for the purposes of analyzing system and storage utilization, problem troubleshooting, and security administration, and in support of audits. Technicians may **not** disclose or permit access to specific information technology resources assigned to, or electronic information associated with, an individual except as authorized under Section 1 above.
   d. **Incident Response** - The incident response function within the University Information Policy Office (UIPO) is responsible for investigating reports of abuse or misuse of university information technology resources. Incident response staff may use system-generated, content-neutral information for the purposes of investigating technology misuse incidents, and in support of audits. Incident response staff may **not** disclose or permit access to specific information technology resources assigned to, or electronic information associated with, an individual except as authorized under Section 1 above.
   e. **Network Communications** - Security engineers of the University Information Security Office (UISO) may observe, capture, and analyze network communications. "Network communications" may contain content

data and in some cases this content may be viewed to complete analysis. If any data must be stored to complete the assigned tasks, it will be stored securely and deleted as soon as possible. Security engineers may **not** disclose content or log data to other persons except as authorized under Section 1 above.

f. **Implied Consent** – Technicians may access, and permit access to, information technology resources and electronic information in situations where a user has requested assistance diagnosing and/or solving a technical problem or where the technician is performing required maintenance or troubleshooting. In these cases, technicians should strive to limit the scope of the access to that which is necessary to address the problem.

5. **Other Provisions**

a. **Advice and Interpretation** - The Chief Information Policy Officer in the Office of the Vice President for Information Technology represents the University CIO for privacy issues related to the IU Bloomington and IUPUI campuses, and is also available to provide advice and policy interpretation to campus CIOs, department management, and any member of the Indiana University community. Technicians receiving requests for access to computer accounts, files, or network traffic by persons other than the account holder, who are not sure how to handle that request within the provisions of this policy, will consult with the Chief Information Policy Officer or the appropriate campus Chief Information Officer (CIO) prior to granting the access.

b. **Legal Requests** - All legal requests or demands for access to information technology resources or electronic information, including all requests under the Indiana Access to Public Records Act and all subpoenas, warrants, court orders, and other legal documents directing that access be afforded to law enforcement agencies or others, must be delivered immediately to the Office of General Counsel. Should such documents be served on individual system technicians or other persons, the documents must be sent immediately to the Office of General Counsel for review. Counsel will review the request or order, and advise the relevant personnel on the necessary response. In the event that a law enforcement agency seeks to execute a search warrant or other order immediately and will not wait for review by the Office of General Counsel, individual system technicians or other persons receiving such orders should not obstruct the execution of the warrant or order, but should document the actions by law enforcement, notify the Office of General Counsel as soon as possible, and take reasonable steps whenever possible to preserve a copy of any data being removed, for appropriate university use.

c. **Expectation of Privacy** - Although the university seeks to create an atmosphere of privacy with respect to information and information technology resources, users should be aware that because IU is a public institution, and members of the University community are engaged in institutional and academic research projects that may require access to certain de-identified user data, and because the university must be able to ensure the integrity and continuity of its operations, use of the university's information resources cannot be completely private. For example, in addition to the types of permissible access described above, when users engage in incidental personal use of their university email accounts, the contents of their email may be subject to disclosure in response to requests under Indiana's "open records" law. Therefore, users of Indiana University information technology resources are hereby notified that they should have no expectation of privacy in connection with the use of those resources beyond the provisions of this policy. Users should also be aware that although the university takes reasonable measures to ensure the privacy of university information technology resources, the university does not guarantee privacy.

d. **Initiating Access** - Persons seeking access to specific information technology resources and/or electronic information assigned to or associated with an individual, that are maintained by University Information Technology Services (UITS), must send those requests to it-incident@iu.edu. Acting for the University CIO, the University Information Policy Office (UIPO) is responsible for ensuring adherence to proper policy and procedures and will coordinate any subsequent approved access.
Persons seeking access to specific information technology resources and/or electronic information assigned to or associated with an individual, that are **not** maintained by University Information Technology Services (UITS), should direct those requests to the technology director of the unit maintaining those resources (on the Bloomington or IUPUI campuses), or the appropriate campus CIO (on the regional campuses). Campus CIOs and unit technology directors are encouraged to consult with the UIPO as needed.

"Persons seeking access" includes system or database administrators or other technicians who need such access to perform their university responsibilities, or who receive requests from others to access those resources or information.

Definitions

Authorized users are people acting within the scope of a legitimate affiliation with the university, using their assigned and approved credentials (ex. network IDs, passwords, or other access codes) and privileges, to gain approved access to university information technology resources. A person acting outside of a legitimate affiliation with the university or outside the scope of their approved access to university information technology resources is considered an unauthorized user. Content-neutral information is information relating to the operation of systems, including information relating to interactions between individuals and those systems. Such information includes but is not limited to operating system logs (i.e., record of actions or events related to the operation of a system or device), user login records (i.e., logs of usernames used to connect to university systems, noting source and date/time), dial-up logs (i.e., connections to university modems, noting source, date/time, and caller id), network activity logs (i.e., connections attempted or completed to university systems, with source and date/time), non-content network traffic (i.e., source/destination IP address, port, and protocol), email logs (i.e., logs indicating email sent or received by individuals using university email systems, noting sender, recipient, and date/time), account/system configuration information, and audit logs (i.e., records of actions taken on university systems, noting date/time). Critical operational necessity is an urgent need that is indispensable or vital to the operation of a unit. Indiana University information technology resources includes all university owned computers, peripherals, and related equipment and software; voice communications infrastructure, peripherals, and related equipment and software; data communications infrastructure, peripherals, and related equipment and software; all other associated tools, instruments, and facilities; and the services that make use of any of these technology resources. The components may be individually controlled (i.e., assigned to an employee) or shared single-user or multi-user; they may be stand-alone or networked components; and they may be stationary or mobile. This also includes university data and files whether stored on university-owned or personally owned equipment. University Chief Information Officer The primary responsibility of the University CIO is the development and use of information technology in support of the university's vision for excellence in research, teaching, outreach, and lifelong learning. The University Information Policy Office represents the University CIO with respect to policy issues related to the IU Bloomington and IUPUI campuses.

Sanctions

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved this could include the offices of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the General Counsel, and/or appropriate law enforcement agencies. See policy IT-02, Misuse and Abuse of Information Technology Resources for more detail.

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

History

- Reviewed December 2011.
- Revised August 17, 2011: changed titles in *Sanctions* section to more accurately reflect current usage.
- Revised July 23, 2010: updated Institutionally Approved Research language.
- Revised March 4, 2010: enhancing language in *Sanctions* section
- Updated procedures section for "Persons affiliated with external entities collaborating with Indiana University" to match academic no-pay process — September 23, 2008

- (1) Updated Alumni email eligibility to reflect new Alumni Association service — March 2, 2007
- Revised March 12, 2006
- Approved May 23, 2006
- Posted as an interim policy November 15, 2000

Related Information

IT-07 Frequently Asked Questions

PennState The Pennsylvania State University Policies Website

ADMINISTRATIVE POLICIES

AD53 Privacy Policy

Policy Status: Active

Subject Matter Expert:
Holly Swires, 814-863-5915, hzl104@psu.edu (mailto:hzl104@psu.edu)

Policy Steward: Vice President for Administration

Contents:

- Purpose
- Definitions
- Scope
- Policy
- Implementation and Exceptions
- Policy Violations
- Further Information
- Cross References

PURPOSE:

To establish a framework for compliance and responsibility regarding privacy and the protection of an individual's personal information.

DEFINITIONS:

Confidentiality - ensuring that information is not disclosed to unauthorized individuals.

Personally Identifiable Information (PII) – Information maintained by the University that can be used to distinguish or trace an individual's identity that specifically includes Social Security Numbers (SSNs), credit card numbers, bank account numbers, Driver's License numbers, state ID numbers, passport numbers, biometric data (including fingerprints, retina/facial images, and DNA profile), or protected health information. These data elements are defined by the University as personally identifiable information.

Privacy Governance Board - The Privacy Governance Board shall consist of the Chief Ethics and Compliance Officer, the Chief Information Security Officer, the Privacy Officer and the Vice President for Human Resources or their delegees, as appropriate. The role of the Privacy Governance Board will be to advise the Executive Vice President and Provost on privacy related matters. Members from individual units may be consulted/added to the Privacy Governance Board on an ad hoc basis, as needed.

Protected Health Information - Individually identifiable health information that is collected from an individual, created or received by a health care provider, health plan, health care clearinghouse, or other employee of one of the Covered Components of the University. This PHI is confidential and must be treated as protected under HIPAA. Protected Health Information relates to the past, present, or future physical or mental health or condition of an

individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.

SCOPE:

This policy is applicable to all members of The Pennsylvania State University community and visitors to the University, including but not limited to students, scholars, faculty, lecturers/instructors, staff, third-party vendors, and others with access to the University's campus and University PII. This policy also applies to all locations and operations of the University, except for Penn State Health and The Pennsylvania College of Technology, which will follow separate policies.

POLICY:

I. Information Privacy

a. General Privacy

The University shall limit the collection, use, disclosure or storage of PII to that which reasonably serves the University's academic, research, or administrative functions, or other legally required purposes. Such collection, use, disclosure and storage shall comply with applicable Federal and state laws and regulations, and University policies, guidelines and standards.

b. Privacy Principles

This Policy is supplemented by Penn State's Privacy Principles that are modeled after the "Privacy by Design" approach and designed to safeguard individuals' privacy and personal information, maintained by the University, consistent across the Penn State community. Penn State's Privacy Principles can be located at https://psu.box.com/v/privacy-principles. (https://psu.box.com/v/privacy-principles)

c. Information That May Be Disclosed to Third Parties

- Legal Requirements: The University may release records in response to a lawful subpoena, warrant, or court order or where such records could be required or authorized by law to be produced or lawfully requested for any other reason, including disclosure to a government agency.
- Authorized Persons: Records may be disclosed to University officials, and authorized individuals performing work for the University who require the information for the performance of their duties.
- Protection of University Interests: The University may disclose information contained in records to protect its legal interest when those records may be related to the actions of an individual that the University reasonably believes may violate or have violated his/her conditions of employment or threaten injury to people or property.
- Collective Bargaining Agreements: Information may be disclosed as required under the terms of a collective bargaining agreement.
- Emergencies: Information may be disclosed if, in the judgment of the designated custodian of such records, disclosure is necessary to protect the health, safety or property of any person.

d. Expectation of Privacy

In the interest of promoting academic freedom and an open, collegial atmosphere, the University recognizes the reasonable privacy expectations of its employees, affiliates, and students in relation to their personal information, including papers, confidential records, and communications by mail, telephone, and other electronic means, subject only to applicable state and federal laws and University policies and regulations, including the policy set forth herein. The University will not monitor such information without cause except as required by law or permitted by University Policy.

e. Applicable Guidelines

In invoking the exception clause ("subject only to applicable state and federal laws and University polices and

regulations"), the following guidelines apply:

1. Necessary Action – Exceptions to the privacy policy may be authorized only when reasonably necessary to protect the security and interests, legal or otherwise, of the University, its communications system, and the academic process, or when there is reason to believe that the individual has violated or may have violated law or University regulations.
2. Consultation – The exception clause may be invoked only by persons with responsibility and authority for administering the law or regulations within the University (e.g., computer security officer, University police) and, except for civil or criminal matters or proceedings, compliance with any other legal requirement, matters of public safety, or when conditions or circumstances exist that necessitate immediate access, only after consultation with an appropriate University Official, as defined in AD83, or the Privacy Governance Board. The Privacy Governance Board's deliberations, when consulted, shall be kept confidential.
3. Notification – Where practicable (and subject to the University's legal obligations, the circumstances described in this and all other University policies, or conditions or circumstances exist that necessitate immediate access), the University shall provide advance notification to an individual prior to all other University access, for cause, to the content of an individual's user files / systems / activity (and, if necessary, physical locations in order to access said files / systems / activity). In certain instances where an individual is, for any reason, unavailable to receive such advance notification and his or her individual data is to be accessed to accomplish legitimate University business, access may also be permitted without prior notification.

f. Responsibility

Executive guidance for the Privacy interests addressed by this policy and related guidelines of both the University and those individuals whose private data has been entrusted to its care shall be vested in the Executive Vice President and Provost.

II. Specific Categories of Information

The below are data use constraints related to certain types of data collected, processed, stored, or published by the University.

EMAIL ADDRESSES - E-mail addresses appearing on University web sites are published for the sole purpose of facilitating private, individual communication between University personnel and readers. The University will not distribute, sell, or otherwise transfer addresses on its website or online services to non-affiliated parties or individuals. The University reserves the right to use internal search functions to obtain specific email addresses for normal business operations. Information such as email addresses may also be displayed in online directories accessible by the general public, unless requested otherwise (see AD11 (/policies/ad11), University Policy on Confidentiality of Student Records and HR58 (/policies/hr58), Employee Office Address and Telephone Number Information).

INFORMATION COLLECTED FOR SERVICE PROVISION – On occasion, the University may collect information from and about users to synchronize systems or update the experience between the user and Penn State. Penn State will not sell, trade, or share the information collected per the University's Web Privacy Statement (http://www.psu.edu/web-privacy-statement). Information collected will be used solely for the purpose for which it was intended.

SOCIAL SECURITY NUMBER (SSN) AND PENN STATE IDENTIFICATION NUMBER (PSU ID) – A Penn State Identification Number (PSU ID) will be assigned to all students and employees of the University as the primary identification number for University purposes. The PSU ID shall be unique to the individual and is a lifetime assignment used for multiple and changing relationships with the University. For more information on the PSU ID, refer to University Policy AD97 (/policies/ad97).

As a matter of University policy, and except as may be required by applicable federal, state or local laws or regulations, it is prohibited that, and in no case shall, any SSN be used as an identifier in a University hosted or developed system or applications, or transmitted electronically, unencrypted. SSNs and/or PII must only be used to accomplish legitimate University business needs or requirements. SSNs will only be requested and required in

certain cases, such as when required by law or for business purposes with certain third party providers.

All records containing PII will be classified, at a minimum, as "High" pursuant to AD95 (/policies/ad95) and must be secured appropriately. Other data elements not specifically classified as PII but that can otherwise be used to distinguish or trace an individual's identity (e.g. Date of Birth) must be classified, at a minimum, as "Moderate" pursuant to AD95 (/policies/ad95), unless an exception (https://psu.app.box.com/v/exception) is approved by the Chief Privacy Officer, privacy@psu.edu (mailto:privacy@psu.edu) and/or the Chief Information Security Officer, security@psu.edu (mailto:security@psu.edu). (See Policy AD95 (/policies/ad95), Information Assurance and IT Security and corresponding standards).

Disposal of the records must be done securely, and in accordance with Policy AD35 (/policies/ad35), University Archives and Records Management.

HEALTH INFORMATION - Individuals have rights with respect to the privacy and security of their health information under Federal and state laws and regulations, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). These rights are outlined in University Policy AD22 (/policies/ad22), Health Insurance Portability and Accountability Act (HIPAA).

INFORMATION COLLECTED FROM UNIVERSITY'S WEBSITE – Information collected on the University's website is governed by the University's Web Privacy Statement (http://www.psu.edu/web-privacy-statement).

ELECTRONIC SECURITY SYSTEM INFORMATION - Access by University units and individuals to information gathered, processed, and archived through electronic security systems (e.g., card or other facility access systems, alarm systems, video surveillance systems) shall occur only in accordance with Policy AD65 (/policies/ad65), Electronic Security and Access Systems.

III. Data Protection and Data Loss Prevention

In order to protect "High" or "Restricted" data entrusted to its care (See Policy AD95 (/policies/ad95), Information Assurance and IT Security and its corresponding standards), the University reserves the right to monitor its networks to detect and respond to externally or internally generated attacks upon its systems, subject to the constraints of this Policy.

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) – All systems that house certain types of information classified as "High," such as PII, are subject to the Pennsylvania Data Security Breach Notification Laws, (PA Statutes, Title 73, Ch. 43, §2301 -2308, 2329) and/or other applicable data breach notification laws. University systems classified as High and Restricted must be scanned appropriately to identify PII using University approved scanning procedures. Users of University systems shall utilize the results of required scanning to facilitate proper handling of any and all PII identified.

University approved scanning procedures will be developed to identify stored PII to facilitate proper handling. Users are responsible for remediating (i.e., securely removing, redacting) unauthorized instances of PII on their systems. If, however, the scanning identifies PII that also is subject to a litigation hold, please contact the Office of General Counsel before remediating. Subject to the constraints of this Policy regarding authorization, the University also reserves the right to perform automated checks to detect and respond to the possible exfiltration of PII over its computer networks. Periodic security scans for PII will be administered to detect unauthorized instances of PII, when necessary. Deliberate failure to remediate unauthorized instances of PII may result in disciplinary action. Please see the following resource (https://security.psu.edu/spirion/) for specific guidance and direction as to current University approved scanning procedures.

Specific details on the permitted use, storage, and transmission of PII, as defined in this Policy, can be located in the below Standard:

PII Standard (https://psu.box.com/v/pii-standard)

This Standard will be enforced in the same manner as this Policy.

VENDOR CONTRACTS – In the event that a unit, department, or individual seeks to enter into a contract that

involves PII, that particular unit, department, or individual is responsible for ensuring that adequate and appropriate safeguards and contractual provisions are in place relating to the collection, access, use, dissemination, and/or storage of this PII before entering the contract. Moreover, before a unit, department, or individual enters into a contract that involves the use of PII, that unit, department, or individual must (1) notify and consult every other unit or department across the University involved, either directly or indirectly, about the necessity for PII in the performance of the contract, (2) seek approval from every other unit or department across the University whose interests in or records of PII may be disclosed or utilized in performance of the contract, and (3) seek approval from the Privacy Office. The applicable safeguards shall be documented in writing in an appropriate manner to ensure compliance.

IMPLEMENTATION AND EXCEPTIONS

Any questions regarding the content of this Policy or supplemental Guidelines and Standards should be referred directly to the Chief Privacy Officer (privacy@psu.edu (mailto:privacy@psu.edu)) who has responsibility to interpret.

POLICY VIOLATIONS

Federal, state, and/or local governments have enacted various laws and regulations relating to privacy to which the University is bound. Compliance with this Policy is designed, in part, to ensure that the University is complying with its various privacy-related obligations.

To the extent any violation of this Policy results in, leads to, or is responsible for a reportable incident or penalties imposed by government regulators or agencies, then that specific department or unit operating in violation of this Policy may be required to cover all University costs associated with the resulting reportable incident and/or associated government penalties.

University employees or students who violate this Policy and/or supplement Guidelines and Standards may be subject to disciplinary action.

FURTHER INFORMATION:

For questions, additional detail, or to request changes to this policy, please contact the Privacy Office.

CROSS REFERENCES:

Other Policies should also be referenced, especially:

AD11 (/policies/ad11), University Policy on Confidentiality of Student Records

AD22 (/policies/ad22), Health Insurance Portability and Accountability Act (HIPAA)

AD35 (/policies/ad35), University Archives and Records Management

AD65 (/policies/ad65), Electronic Security and Access Systems (formerly SY33)

AD83 (/policies/ad83), Institutional Financial Conflict of Interest

AD95 (/policies/ad95), Information Assurance and IT Security

AD96 (/policies/ad96), Acceptable Use of University Information Resources

HR60 (/policies/hr60), Access to Personnel Files

RA02 (/policies/rp02), Addressing Allegations of Research Misconduct (Formerly RA10, Handling Inquiries/Investigations Into Questions of Ethics in Research and in Other Scholarly Activities)

RP07 (/policies/rp07), HIPAA and Research at Penn State University

Most recent changes:

- May 30, 2018 - Updates include incorporating a Standard, the adoption of the Privacy Principles, updates to language on PII scanning, addition of sections on Implementation and Exceptions and Policy Violations, and retiring ADG08.

Revision History (and effective dates):

- September 18, 2017 - Editorial changes and updates to the definition of PII.
- February 22, 2016 - Major changes to the entire document to reflect the reorganization of University privacy policies.
- August 1, 2007 - Changes to POLICY section.
- August 28, 2003 - Significant rewrite emphasizing the balance between privacy issues and the need to observe state and federal laws and University regulations.
- February 22, 2000 - New Policy.

Date Approved: May 30, 2018

Date Published: May 30, 2018

Effective Date: May 30, 2018

IRM-012: Privacy and Confidentiality of University Information

Date: 10/23/2017 Status: Final
Last Revised: 10/23/2017
Policy Type: University
Contact Office: University Information Security (InfoSec)
Oversight Executive: Chief Information Officer
Applies To: Academic Division, the Medical Center, the College at Wise, and University-Related Foundations.
Table of Contents:

Policy Statement

I. Monitoring and Access
   1. Monitoring and/or Access without further Authorization or Notification
   2. Monitoring and/or Access Requiring Official University Review and Approval
   3. Accessing Electronically Stored Information of a Deceased Person

II. Compliance with Policy

Procedures

Reason for Policy:

The University may access *records* or monitor *record systems or communications* that are under the control of its employees. Furthermore, because the University permits some latitude for employees to use University resources to conduct University business off-grounds and to conduct incidental personal matters at their work sites, *work-related records* and employees' *personal records* may be located in the same place.

The University is committed to the privacy of individuals and safeguarding information about individuals subject to limitations imposed by local, state, and federal law and other provisions described herein.

No user has any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the Commonwealth's equipment and/or access. The University has the right to monitor any and all aspects of their computer systems and to do so at any time, without notice, and without the user's permission.

The University holds as core values the principles of academic freedom and free expression. This policy takes into consideration these principles.

Definition of Terms in Statement:

- Access (to data):

  The capacity for data users to enter, modify, delete, view, copy, or download data.

- Data Users:

  Individuals who acknowledge acceptance of their responsibilities, as described in this policy, and its associated standards and procedures, to protect and appropriately use data to which they are given access; and meet all prerequisite requirements, e.g., attend training before being granted access.

- Authorizing Official (2):

  An individual at the University who is authorized to grant a request to access Electronically Stored Information (ESI). This may include an individual who has been designated, either permanently or temporarily, by another individual to serve in the role of authorizing official on their behalf. The authorizing official (a.k.a approver) typically would be from within the same department, business unit, or reporting area, and must be at least two levels above the affected individual(s) on an organizational chart (except where the affected individual is the president or vice-president). The authorizing official is a person in a higher-level position of authority who is able to determine appropriateness and reasonableness after reviewing the applicable policies and standards related to the request. For most situations, the authorizing official will be either the department chairs or heads or their assigned designee, or the President or delegated representative, such as the Vice-Presidents and Deans or their assigned designee, depending on the affected user and requested access.

- Electronic Communications:

  Includes telephone communications, so-called "phone mail," or voicemail, e-mail, computer files, text files, and any data traversing the University network or stored on University equipment.

- Electronically Stored Information (ESI):

  Information created, manipulated, stored, or accessed in digital or electronic form.

- Employee (5):

  An individual who is an *employee (2)*, *contractor employee*, *medical center employee,* and/or *foundation employee*, as well anyone else to whom University IT resources have been extended. These include, but are not limited to, recently terminated employees whose access to University IT resources have not yet been terminated, deleted, or transferred, and individuals whose University IT resources continue between periods of employment. This also includes student workers, volunteers, and other individuals who may be using state-owned or University IT resources and carrying out University work.

  - Contractor Employee:

    An individual who is an employee of a firm that has a formal contractual relationship with the University and has been assigned to work at the University for the duration of the contract.

  - Employee (2):

    As used in this policy, includes all faculty (teaching, research, administrative and professional), professional research staff, university and classified staff employed by the University in any capacity, whether full-time or part-time, and all those employees in a wage or temporary status.

  - Foundation Employee:

    An individual who is an employee of one of the officially recognized University-related foundations.

  - Medical Center Employees:

    Individuals employed by the University of Virginia Medical Center in any capacity.

- Information Technology (IT) Resources:
  All resources owned, leased, managed, controlled, or contracted by the University involving networking, computing, electronic communication, and the management and storage of electronic data regardless of the source of funds including, but not limited to:
  - Networks (virtual and physical), networking equipment, and associated wiring including, but not limited to: gateways, routers, switches, wireless access points, concentrators, firewalls, and Internet-protocol telephony devices;
  - Electronic devices containing computer processors including, but not limited to: computers, laptops, desktops, servers (virtual or physical), smart phones, tablets, digital assistants, printers, copiers, network-aware devices with embedded electronic systems (i.e., "Internet of things"), and supervisory control and data acquisition (SCADA) and industrial control systems;
  - Electronic data storage devices including, but not limited to: hard drives, solid state drives, optical disks (e.g., CDs, DVDs), thumb drives, and magnetic tape;
  - Software including, but not limited to: applications, databases, content management systems, web services, and print services;
  - Electronic data in transmission and at rest;
  - Network and communications access and associated privileges; and
  - Account access and associated privileges to any other IT resource.
- Inquiry:

  Gathering information and initial fact-finding to determine whether an allegation or apparent instance of research misconduct warrants an investigation.
- Investigation:

  The formal examination and evaluation of all relevant facts to determine if misconduct has occurred, and, if so, to determine the responsible person and the seriousness of the misconduct.
- Protected Information:

  Refers to information that is linked to a person's identity, such as Social Security Number (SSN), driver's license number, financial information, and/or protected health information (PHI).
- Record:

  Any document, file, computer program, database, image, recording, or other means of expressing information in either electronic or non-electronic form.
- University Record:

  Recorded information that documents a transaction or activity by or with any appointed board member, officer, or employee of the University. Regardless of physical form or characteristic, the recorded information is a University record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of university business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is a University record. University records include but are not limited to: personnel records, student records, research records, financial records, patient records and administrative records. Record formats/media include but are not limited to: email, electronic databases, electronic files, paper, audio, video and images (photographs).
  - Research Record:

    One type of University record that includes, but is not limited to: grant or contract applications, whether funded or unfunded; grant or contract progress and other reports; laboratory notebooks; notes; correspondence; videos; photographs; X-ray film; slides; biological materials; computer files and printouts; manuscripts and publications; equipment use logs; laboratory procurement records;

animal facility records; human and animal subject protocols; consent forms; medical charts; and patient research files. In addition, research records include any data, document, computer file, computer diskette, or any other written or non-written account or object that reasonably may be expected to provide evidence or information regarding the proposed, conducted, or reported research that constitutes the subject of an allegation of research misconduct.

- User:

  Everyone who uses University information technology (IT) resources. This includes all account holders and users of University IT resources including, but not limited to: students, applicants, faculty, staff, medical center employees, contractors, foundation employees, guests, and affiliates of any kind.

Policy Statement:

The University, as steward of public resources and electronic information, shall respond to requests for electronic information in an orderly manner consistent with state and federal law. This policy applies to all users of the University's information technology resources, regardless of location or affiliation.

Release of Information: Except as provided below, the University may not release protected information about any aspect of an individual's association with the University without the prior written consent of the individual concerned or unless legally required (e.g., Virginia Freedom of Information Act (FOIA) or legal request). Within the University, access to such records shall be restricted to authorized personnel for authorized reasons, as determined by the President or his/her delegated representative, such as the Vice-Presidents and Deans, and such others as are agreed to in writing by the individual concerned.

Except as provided below, the employees of the University will not monitor the content of electronic communications of its users including personal and University records, files, and data, nor will it examine the content of a user's electronic communications or other electronic files stored on its systems except under certain circumstances**.**

I. **Monitoring and Access:**
   1. **Monitoring and/or Access without further Authorization or Notification:** Legal or administrative circumstances where monitoring and/or access may occur without further authorization or notification include:
      - Communications or files subject to legal orders or demands (e.g., subpoena, warrants, and national security letter) or requested in accord with FOIA.
      - Supervisor and/or Internal Audit review of University telephone system local or long-distance call records.
      - Electronic communications or files that have been inadvertently exposed to technical staff who are operating in good faith to resolve technical problems. When technical staff inadvertently discovers potentially illegal content in communications or files, they are required to report it. Otherwise, the University expects technical staff to treat inadvertently encountered electronic communications and files of users as confidential.
      - Routine administrative functions, such as security tests to maintain and/or verify the security and/or integrity and/or availability of the University's IT resources, e.g., password testing to identify guessable passwords, investigations of attempted access into systems by unauthorized persons, or email scanning for malware. See policy IRM-004, Information Security of University Technology Resources for additional details.
      - Officially sanctioned research projects or projects authorized by the University to be conducted under a data use agreement that limits the disclosure of protected information.
      - To the extent permitted by law, the University may disclose, to an alleged victim of any crime of violence (as that term is defined in section 16 of title 18, United States Code), the results of any disciplinary proceeding conducted by the University against the alleged perpetrator of such crime with respect to such crime.

2. **Monitoring and/or Access Requiring Official University Review and Approval:**
   Circumstances where monitoring and/or access requires official University review and approval by an authorizing official who is the President or the relevant vice president (or delegate) responsible for the affected user (e.g., employee or student):
   - Business continuity of the University to proceed [e.g., access to data associated with a user (e.g., employee) who has been terminated, separated, is pending termination or separation, is deceased, is on extended sick leave, or is otherwise unavailable].
   - An inquiry, assessment, or investigation into violation(s) of law or policy, or in response to potential or actual litigation.
   - Requests for electronically stored information (ESI) from members of the University's Honor Committee or Judiciary Committee, the Title IX Coordinator and/or designee acting under the University's Policy on Sexual and Gender-Based Harassment and Other Forms of Interpersonal Violence, or faculty conducting individual student-academic-issue investigations.
   - Emergency situations involving a potential threat of harm to persons or property as determined by an authorizing official who is the President or the relevant vice president (or delegate) in consultation with University Counsel.
   - Those units of the University that engage in routine monitoring or examination of employee(s) electronic communications or files as part of the work environment must inform the affected employee(s) in advance, via a written communication (e.g., policy statement) that such monitoring or examination will be taking place.

3. **Accessing Electronically Stored Information of a Deceased Person:**
   The University will not grant access to data from a deceased user's electronically stored information in the custody of the University without the prior written consent of the deceased individual concerned or unless allowed or required by law or legal requests [e.g., Freedom of Information Act (FOIA), Uniform Fiduciary Access to Digital Assets Act (UFADA)].

II. **Compliance with Policy:**
Any misuse of data or IT resources may result in limitation or revocation of access to University IT resources. In addition, failure to comply with requirements of this policy and/or its standards may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may also violate federal, state, or local laws.

Questions about this policy should be directed to the Contact Office.

Procedures:

Privacy and Confidentiality	
Standards and Procedures	
Standards	**Procedures**
ESI Release	ESI Release
	Exceptions

Responsible Computing Handbook for Faculty and Staff

Related Information:

See related Guidance for Vice Presidents on Policy on Monitoring/Review of Employee Electronic Communications or Files document

The Commonwealth of Virginia Human Resource Policy 1.75

Commonwealth of Virginia Freedom of Information Act (FOIA)

Stored Wire and Electronic Communications And Transactional Records Access

Uniform Fiduciary Access to Digital Assets Act (UFADA)

Major Category: Information Resource Management
Next Scheduled Review: 10/23/2020
Approved by, Date: Policy Review Committee, 06/27/2017
Supersedes (previous policy):
Employee Electronic Communication/File Monitoring and/or Review; Virginia.edu Privacy Statement; Information Release (Requests for Electronically Stored Information).

Source URL: http://uvapolicy.virginia.edu/policy/IRM-012

Official Student Record Information Privacy Policy

OFFICIAL STUDENT RECORD INFORMATION PRIVACY POLICY

Contents

1. Purpose
2. Definitions and General Principles
3. Information Contained in Official Student Records
4. Access to and Disclosure of Information:
   (a) "Public" Personal Information
   (b) Prospective Applicants and Applicants
   (c) Current Students
   (d) Next of Kin
   (e) Faculty and Staff
   (f) Alumni/ae and Former Students
   (g) University Student Organizations
   (h) Affiliated College and Other Institutions
   (i) Agents of the University
5. Custody, Storage and Retention of Official Student Record Information

1. Purpose

This document sets out the University's policy on the collection, use and disclosure of the personal information that forms part of the Official Student Record and the personal information collected on prospective applicants and applicants who do not become students. It applies to the Office of the Registrar, the Faculty of Graduate Studies, and all other academic and administrative units that are the primary and secondary custodians of specified data collected and stored about prospective applicants, applicants, students, alumni/ae and former students of the University.

2. Definitions and General Principles

For the purposes of this policy:

(a) *prospective applicant* means a person who has indicated an interest in applying for admission to the University and/or who has been identified by the University as a person who will be considered for recruitment (e.g. major scholarship winners);

(b) *applicant* means any person who has formally applied for admission to the University and whose application is still active;

(c) *current student* means any person who is active in the current term and/or active in any program at the University *[A student is considered to be active in the current term if he or she has taken some action, such as completing registration, paying a tuition deposit or a portion of term tuition fees, or completing an add/drop. A student is considered active in a program within a period of 2 years of being active in a term]*;

(d) *alumnus or alumna* means any person who has received a degree, diploma or certificate from the University and is not active in a program *[For the purposes of this policy a Western graduate who is also a current student is considered a*

current student.]; and

(e) *former student* means any person who has attended the University but has not received a degree, diploma or certificate and is not active in a program.

During the University recruitment process, information will be collected and used to identify prospective applicants who will be encouraged to apply for admission to the University.

During the admission process, information will be collected and used to establish a record and assess an applicant's qualification for admission to the University.

During the registration process and the student's subsequent academic career, specific information that constitutes the Official Student Record will be collected, maintained and used by the University to:

- record performance in programs and courses;
- record decisions of academic appeals/petitions and scholastic and non-academic offence decisions and sanctions;
- provide the basis for financial aid, awards and government funding; and,
- assist the University in the academic and financial administration of its affairs which, for example, can range from the day-to-day administration of academic programs to long-range financial or capital planning.

All documentation submitted to the University in support of an application for admission, residence accommodation, or financial award, or as part of any investigation, appeal/petition or request, becomes the property of the University.

Other than disclosure of information specified in Section 4(a) below, the University is committed to taking every reasonable step to protect the confidentiality and privacy of the information contained in the Official Student Record or collected on prospective applicants and applicants who do not become students. Such information must not be disclosed to any individual or institution outside the University, its Affiliated Colleges, or organizations offering joint programs, placements, internships, etc., as part of a course or program at the University, except in the following circumstances:

- with the student's consent (written preferred);
- under compulsion of law;
- in accordance with the requirements of professional licensing or certification bodies;
- pursuant to an investigation of possible misrepresentation concerning an individual's references, attendance, performance, status within, or completion of an academic program at the University or at another academic institution;
- in compassionate or emergency situations, as determined by the custodian of the information; and
- in other circumstances set out in the University's *Guidelines on Access to Information and Protection of Privacy* [hereafter *Guidelines on Access*] or as permitted under applicable federal or provincial legislation.

The University will maintain a record of all occasions on which Official Student Record information, other than information specified in Section 4(a), is provided to a third party in the absence of the consent of the student. The contents of this record will be available to the student upon request unless disclosure of the information would compromise an ongoing University or criminal investigation, or is otherwise prohibited by

law.

General statistical material drawn from academic records that does not disclose the identities of prospective applicants, applicants, students, alumni/ae or former students may be released for research and information purposes authorized by the University.

3. Information Contained in Official Student Records

Official Student Records, in electronic or paper form, contain the following information relating to a student's application, admission, and performance at the University:

(a) personal information (name, address, e-mail address, telephone, date of birth, citizenship, social insurance number, student number, photograph, etc.);
(b) basis of admission information (application, record of previous studies, letters of recommendation, test results, etc.);
(c) registration and enrollment information (programs of study, dates of attendance, academic load, courses taken, credits transferred, etc.);
(d) performance information (grades, averages and ranks, narrative evaluations, clinical evaluations, distinctions/awards, special permissions, academic counselling information, degrees obtained, requirements to withdraw, scholastic offence decisions[1], etc.);
(e) decisions relating to academic appeals/petitions;
(f) decisions against a student, including appeal decisions, under the Code of Student Conduct;
(g) medical information given to a Faculty related to a student's performance that is provided by or collected with the consent of the student; and
(h) financial information (tuition fees and other charges, payments, awards, debts, etc.).

The following information is not considered to form part of the Official Student Record and is not covered by the provisions of this policy:

- medical information provided to Student Health Services;
- information relating to the employment by the University of current students, alumni/ae or former students; and
- information other than basic demographic data that is maintained by or on behalf of Alumni Affairs and Development and which is deemed to constitute the Official Alumni Record.

4. Access to and Disclosure of Information

(a) "Public" Personal Information

It is the practice of the University to consider the following information to be publicly available and to provide it to third parties in response to requests (e.g., confirmation of information for a potential employer) without first seeking the consent of the individual each and every time a request is received:

- Full name
- Degree(s) awarded by Western and date(s) conferred, if applicable

[1] Access to and disclosure of any information relating to a scholastic offence that is not recorded on a student's transcript, such as a decision letter, is governed by Senate regulations and not this policy (see "Release of Information Concerning Scholastic Offences" in the Academic Calendar).

- Faculty(ies)/Schools in which student is/was enrolled, with major field of study
- Academic or other University honors or distinctions

However, at any time an individual may request that this information cease to be made publicly available by contacting the Office of the Registrar or the Faculty of Graduate Studies, as appropriate, in writing.

(b) Prospective Applicants and Applicants

Prospective Applicants and Applicants may, upon written request, be granted limited access to records containing their personal information in accordance with the Access Procedure set out in Section 6 of the *Guidelines on Access.* Access will not be provided to records that have been submitted to the University in confidence either implicitly or explicitly (e.g., letters of reference), that document deliberative processes, or are otherwise exempt under the *Guidelines on Access.* Outdated records for prospective applicants, records for unsuccessful applicants, and records for those who do not accept an offer of admission, are not retained indefinitely. They will be destroyed in accordance with approved retention and disposal schedules.

(c) Current Students

Current students normally have access to their Official Student Record, except material submitted to the University in confidence (e.g., letters of reference) or otherwise exempt from access under the *Guidelines on Access*, by making an informal request to the appropriate University office. However, students may also request access in accordance with the Access Procedure set out in Section 6 of the *Guidelines on Access*. If a student has outstanding debts to the University, access may be restricted and certain academic documents (e.g., transcripts, graduation diplomas) may be withheld until payment is received.

(d) Next of Kin

Next of kin will not be given access to information in the Official Student Record except as provided for in Section 2 above, the most common circumstance being with the prior consent of the student. This provision applies regardless of the age of the student (i.e., whether or not they are under the age of 18) as it is the student's ability to consent, rather than their age, that is the determining factor in their right to exercise control over their own personal information.

(e) Faculty and Staff

Within the University, access to the Official Student Record is restricted to faculty and staff who have a legitimate need for the information in order to carry out the responsibilities of their position or office as it relates to the administration of student affairs and services. For example, access to information contained in the Official Student Record of current students, former students or alumni/ae who are also employees of the University will not be provided for employment related purposes without the prior consent of the individual. Similarly, details of medical information supplied to Faculty offices will not be released without the prior consent of the individual.

Access to financial assistance information of the Ontario Student Assistance Program, to other forms of assistance based on financial need, or to individual

earnings is restricted to financial aid staff in the Office of the Registrar, and to a limited number of authorized staff in the Faculty of Graduate Studies, Housing and Ancillary Services, Deans' and other administrative offices. Relevant information is routinely provided to government agencies with a legitimate need to know, such as those involved in the administration of scholarship or financial aid programs.

The Department of Advancement Services and the Department of Alumni Relations and Development will be permitted access to personal information relating to the identity and location of prospective applicants, applicants and students in order to maintain contact with the individuals and inform them of events, programs and services.

Ensuring the security and privacy of personal information is a collective responsibility of the Office of the Registrar and Faculty of Graduate Studies, and the Deans, Chairs, Directors and managers of academic and administrative units. All full-time and part-time faculty and staff who receive this information must be formally notified of the contents of the Policy, the requirement to adhere to its provisions, and the implications of non-compliance.

E-mail often provides the most efficient and timely medium for communicating with students, prospective applicants, applicants, former students and alumni/ae. However, personal information should not normally be communicated electronically. Where such communication is necessary, a reasonable effort will be made to correctly identify the requester and/or recipient prior to sending personal information.

(f) Alumni/ae and Former Students

An alumnus, alumna or a former student may request access to his or her Official Student Record in accordance with the Access Procedure set out in Section 6 of the *Guidelines on Access*.

(g) University Student Organizations

Student organizations recognized by the Board of Governors (i.e., the University Students' Council, Society of Graduate Students, and MBA Association) shall have access to basic student information referred to in Sections 3(a) and (c), for the legitimate internal use of that organization. The disclosure of such information will be subject to agreements with the organizations that they will not disclose any information to a third party, or use the information for any commercial purpose, without the prior agreement of the University.

The USC, SOGS, and the MBAA shall be entitled to publish and distribute within the University community a University-wide directory of students except where students have restricted the disclosure of information. Students wishing to restrict the disclosure of information may do so by contacting the organization.

Student information will not be released to student clubs or organizations not recognized by the Board of Governors without the consent of the students. However, the University will make reasonable efforts to facilitate communication between these groups and individual students. For example, under certain circumstances an information package prepared by a club could be distributed directly to students by the University on behalf of the club, in lieu of giving the

club access to student addresses.

(h) Affiliated Colleges and Other Institutions

The University will disclose information in an Official Student Record to its Affiliated Colleges on a need to know basis and in accordance with the terms of the Affiliation Agreement between the University and its Affiliated Colleges. In addition, the University will disclose information in an Official Student Record to other institutions to the extent required for a particular course or program (e.g. off-campus placements, internships, joint programs).

(i) Agents of the University

The University may contract with external agents for the provision of goods or services. These agents may range in size from nation-wide companies to individuals providing volunteer support. As part of the arrangements between the University and the agent, there may be a requirement to disclose certain student information to the agent. However, any such disclosure will be governed by a confidentiality agreement between the University and the agent that specifies the purpose(s) of the disclosure and the University's expectations with respect to confidentiality.

5. Custody, Storage and Retention of Official Student Records

The University maintains Official Student Records in electronic or paper form. Electronic records contain information required to monitor the progress and performance of students, produce periodic performance reports, and provide attestations of achievement and official transcripts of academic records. They also form the basis of management information needed for the operation of the University and for enrollment reports and statistical information required by government agencies. All portions of the electronic student academic record needed to produce official transcripts are maintained indefinitely. As these records are retained on a permanent basis they will be reviewed periodically, especially at times of an upgrade of the electronic records system or migration to a new system. Metadata pertaining to the system itself will be maintained in hard copy form in the University Archives. Other information in electronic and paper form is retained or disposed of according to the Disposition and Retention Schedules prepared in consultation with the University Archives.

Data Security Policies

Title: **Data Security Policy**
Code: **1-100-200**
Date: **12-31-10rev**
Approved: **WPL**

INTRODUCTION

The purpose of this policy is to outline essential roles and responsibilities within the University community for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests and to establish a comprehensive data security program in compliance with applicable law. This policy is also designed to establish processes for ensuring the security and confidentiality of confidential information and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information.

SCOPE

This policy applies to all Boston College faculty and staff, whether full- or part-time, paid or unpaid, temporary or permanent, as well as to all other members of the University community. This policy applies to all information collected, stored or used by or on behalf of any operational unit, department and person within the community in connection with University operations. In the event that any particular information at Boston College is governed by more specific requirements under other University policies or procedures (such as the policy concerning Student Education Records), the more specific requirements shall take precedence over this policy to the extent there is any conflict.

DEFINITIONS

Information Resource. An Information Resource is a discrete body of information created, collected and stored in connection with the operation and management of the University and used by members of the University having authorized access as a primary source. Information Resources include electronic databases as well as physical files. Information derived from an Information Resource by authorized users is not an Information Resource, although such information shall be subject to this policy.

Sponsors. Sponsors are those members of the University community that have primary responsibility for maintaining any particular Information Resource. Sponsors may be designated by a Vice President or Dean in connection with their administrative responsibilities (as in the case of the University Registrar with respect to student academic records), or by the actual sponsorship, collection, development, or storage of information (as in the case of individual faculty members with respect to their own research data, or student grades).

Data Security Officers. Data Security Officers are those members of the University community, designated by their University Vice President or Dean, who provide administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific Information Resources in consultation with the relevant Sponsors.

Users. Users include virtually all members of the Boston College community to the extent they have authorized access to University Information Resources, and may include students, faculty, staff, contractors, consultants and temporary employees and volunteers.

Data Security Committee. The Data Security Committee shall be chaired by the Executive Vice President and shall include the following Vice Presidents or their representatives: the Provost, the Financial Vice President and Treasurer, the Vice President for Information Technology, the Vice President for Human Resources, and the General Counsel.

Computer System Security Requirements. Computer System Security Requirements shall mean a written set of technical standards and related procedures and protocols designed to protect against risks to the security and integrity of data that is processed, stored, transmitted, or disposed of through the use of University information systems, and shall include computer system security requirements that meet or exceed the requirements of regulations promulgated under Chapter 93H of Massachusetts General Laws. The Computer System Security Requirements shall be set forth as an exhibit hereto. The Computer System Security Requirements establish minimum standards and may not reflect all the technical standards and protocols in effect at the University at any given time.

Data Security Directives. Data Security Directives shall be issued from time to time by the Data Security Committee to provide clarification of this policy, or to supplement this policy through more detailed procedures or specifications, or through action plans or timetables to aid in the implementation of specific security measures. All Data Security Directives issued by the Committee shall be deemed incorporated herein.

Specific Security Procedures. Specific Security Procedures are procedures promulgated by a University Vice President or Dean to address particular security needs of specific Information Resources sponsored within their area of responsibility, not otherwise addressed by this policy, or any Data Security Directives.

Data Security Working Group. The Data Security Working Group shall be chaired by the Director of Computer Policy and Security, and shall consist of those Data Security Officers as may be assigned to the group from time to time by the Data Security Committee.

Security Breach. A Security Breach is any event that causes or is likely to cause Confidential Information to be accessed or used by an unauthorized person and shall include any incident in which the University is required to make a notification under applicable law, including chapter 93H of the Massachusetts General Laws.

DATA CLASSIFICATION

1. All information covered by this policy is to be classified among one of three categories, according to the level of security required. In descending order of sensitivity, these categories (or "security classifications") are "*Confidential*," "*Internal Use Only*," and "*Public*."

- *Confidential* information includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal Confidential information may result in a significant invasion of privacy, or may expose members of the University community to significant financial risk. Unauthorized access or modification to institutional Confidential information may result in direct, materially negative impacts on the finances, operations, or reputation of Boston College. Examples of personal Confidential information include information protected under privacy laws (including, without limitation, the Family Educational Rights and Privacy Act and the Gramm-Leach-Bliley Act), information concerning the pay and benefits of University employees, personal identification information or medical/health information pertaining to members of the University community, and data collected in the course of research on human subjects. Institutional Confidential information may include University financial and planning information, legally privileged information, invention disclosures and other information concerning pending patent applications.

  Without limiting the generality of the foregoing, Confidential information shall include "personal information" as defined by Massachusetts General Laws Chapter 93H ("Massachusetts PI"). Massachusetts PI means a Massachusetts resident's first name or first initial and last name in combination with any one or more of the following: (a) social security number; (b) driver's license number or state –issued identification number; (c) financial account number, or credit card or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to the resident's financial account and Confidential information also includes "customer information," defined by the safeguards rule under the Gramm-Leach-Bliley Act to mean any information containing personally identifiable information that the University obtains in the process of offering a financial product or service.

- *Internal Use Only* information includes information that is less sensitive than Confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of Boston College. Examples of this type of data from an institutional perspective include internal memos meant for limited circulation, or draft documents subject to internal comment prior to public release.

- *Public* information is information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual members of the University community or upon the finances, operations, or reputation of Boston College.

2. All Information Resources, whether physical documents, electronic databases, or other collections of information, are to be assigned to a security classification level according to the most sensitive content contained therein.

3. Where practicable, all data is to be *explicitly classified,* such that Users of any particular data derived from an Information Resource are aware of its classification.

4. In the event information is not explicitly classified, it is to be treated as follows: Any data which includes any personal information concerning a member of the University community (including any health information, financial information, academic evaluations, social security numbers or other personal identification information) shall be treated as Confidential. Other information is to be treated as Internal Use Only, unless such information appears in form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.

5. The Data Security Committee may from time to time provide clarifications relating to the security classifications, and may, through issuance of Data Security Directives establish more detailed requirements concerning the classification of Information Resources or specific data.

ROLE OF THE DATA SECURITY WORKING GROUP

1. The University has established the Data Security Working Group to aid in the development of procedures and guidelines concerning the collection, storage, and use of data by the University community, and to assist the Data Security Committee in the implementation of this policy.

2. In consultation with the Office of the General Counsel and the Director of Internal Audit, the Data Security Working Group shall:

- Monitor federal, state and local legislation concerning privacy and data security.

- Stay abreast of evolving best practices in data security and privacy in higher education, and assess whether any changes should be made to the Computer System Security Requirements.

- Establish data privacy and security training and awareness programs for the University community and periodically assess whether these programs are effective.

- Periodically reassess this policy to determine if amendments are indicated or if Data Security Directives should be proposed to the Data Security Committee.

- Discuss any material violations of this policy and Security Breaches, the University's actions in response, and recommend any further actions or changes in practice or policy to the Data Security Committee.

BOSTON COLLEGE
Data Security Policy
http://www.bc.edu/content/dam/files/offices/policies/pdf/policies/I/1-100-200.pdf

ROLE OF THE DATA SECURITY COMMITTEE

1. The University has established the Data Security Committee to formulate University-wide procedures and guidelines concerning the collection, storage, use and safekeeping of data, to update as necessary this policy, and to direct the responsive actions in the event of any material violation of this policy or any Security Breach.

2. The Data Security Committee shall from time to time consult with representatives of the Data Security Working Group to review the implementation of this policy and compliance with the Computer System Security Requirements and Data Security Directives.

3. The Data Security Committee shall periodically review identifiable risks to the security, confidentiality, and integrity of data, and shall review this policy and the scope of Computer System Security Requirements at least annually to assess its effectiveness and determine whether any changes are warranted.

4. The Data Security Committee is authorized to:

- Issue Data Security Directives.
- Promulgate amendments to this policy, including the Computer System Security Requirements.
- Take actions to ensure compliance with this policy, which may include, without limitation, the commissioning of internal audits and investigations.
- Take actions in response to violations of this policy or any Security Breach.

ROLE OF THE DIRECTOR OF COMPUTR POLICY AND SECURITY

1. The Director of Computer Policy and Security shall, with input from the Data Security Working Group, identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of University data. This identification and risk assessment shall include adopting means for detecting security system failures and monitoring the effectiveness of the Computer System Security Requirements.

2. The Director shall, in conjunction with the Data Security Working Group, oversee the implementation of the Computer System Security Requirements and recommend changes to address risks, failures, or changes to business practices to the Data Security Committee.

3. The Director shall work with other University administrators to investigate any violation of this policy and any incident in which the security or integrity of University data may have been compromised, including taking the steps set forth below in response to a security breach.

4. The Director shall work with other University administrators to develop and review training materials to be used for employee training under this policy.

SECURITY RESPONSIBILITIES

1. It is the policy of the University that all confidential and other sensitive information be safeguarded from unauthorized access, use, modification or destruction. All members of the University community share in the responsibility for protecting the confidentiality and security of data. This section of the policy assigns specific duties to each of the roles of Vice President and Deans, Sponsors, Data Security Officers, Users, and the Vice President for Human Resources. However, it is likely that an individual will have responsibilities reflecting multiple roles with respect to certain information.

2. *Vice Presidents and Deans*. University Vice Presidents and Deans (including the University President, and the University Provost and Dean of Faculties in connection with their immediate staff) are responsible for promoting the institutional awareness of this policy and for ensuring overall compliance with it by their staff. In particular, Vice Presidents and Deans are responsible for:

- Ensuring that all staff have the training and support necessary to protect data in accordance with this policy, all Data Security Directives, and any Specific Security Procedures applicable to such data.

- Designating and managing the efforts of one or more Sponsors and Data Security Officers for all Information Resources maintained in their area of responsibility.

- Approving access authorization of all Users of Information Resources maintained in their area of responsibility having a data classification of Confidential.

- Promulgating Specific Security Procedures.

- Ensuring that Confidential or Internal Use Only data sponsored within their area of responsibility are not provided or accessible to, or created or maintained by University vendors or other third-parties without (i) assistance from the Director of Computer Policy and Security and the Director of Internal Audit, verifying that the third party has the capability of adequately protecting such data; (ii) review and approval of the relevant contract and the underlying terms and specifications by the Director of Computer Policy and Security and the Office of the General Counsel; and (iii) unless approved otherwise by the Office of the General Counsel, verifying that the third party has executed the University's standard form of Privacy and Security Addendum.

3. *Sponsors*. A Sponsor has primary responsibility for overseeing the collection, storage, use and security of a particular Information Resource. In cases where a Sponsor is not identified for any Information Resource, the cognizant Vice President or Dean shall be deemed the Sponsor. A Sponsor is responsible for the following specific tasks associated with the security of the information:

- Ensuring that the Information Resource is assigned a security classification and that such data is marked where appropriate.

- Identifying authorized Users of the Information Resource, whether by individual identification of by job title, and obtaining approval for such access from their Vice President or Dean.

- Proposing to their Vice President or Dean Specific Security Procedures for the handling of data under their sponsorship, consistent with this policy and other applicable University policies and procedures.

4 *Data Security Officers*. A Data Security Officer works with Information Technology and other appropriate University functions under the direction of a Vice President or Dean and in consultation with a Sponsor, to support the implementation and monitoring of security measures associated with the management of Information Resources. Data Security Officers shall be responsible for:

- Ensuring adequate security technology is applied to Information Resources in keeping with their classification and to comply with this policy and all Data Security Directives, and Specific Security Procedures.

- Monitoring for indicators of loss of integrity.

- Promptly reporting to the Director of Computer Policy and Security any incidents of data being accessed or compromised by unauthorized Users, and any violations of this policy, Data Security Directives or Specific Security Procedures.

- Monitoring for risks to data security and reporting any known or reasonably foreseeable risks to the Data Security Working Group.

5. *Users.* Users are responsible for complying with all security-related procedures pertaining to any Information Resource to which they have authorized access or any information derived therefrom that they possess. Specifically, a *User* is responsible for:

- Becoming familiar with and complying with all relevant University policies, including, without limitation, this policy, and all Data Security Directives contemplated hereby, the policy on Professional Standards and Business Conduct, and other policies related to data protection, technology use and privacy rights (including the University Student Education Records).

- Providing appropriate physical security for information technology equipment, storage media, and physical data. Such equipment and files shall not be left unattended without being locked or otherwise protected such that unauthorized Users cannot obtain physical access to the data or the device(s) storing the data.

- Ensuring that Confidential or Internal Use Only information is not distributed or accessible to unauthorized persons. Users must not share their authorization passwords under any circumstances. Users must avail themselves of any security measures, such as encryption technology, security updates or patches, provided by Data Security Officers. Users must log off from all applications, computers and networks, and physically secure printed material, when not in use.

- To the extent possible, making sure that any Massachusetts PI accessed by the User is stored only on secure servers maintained by the University and not on local machines, unsecure servers, or portable devices.

- Boston College Confidential or Internal Use Only data, when removed from the campus or when accessed from off-campus, is subject to the same rules as would apply were the data on campus. Sponsors and Users will comply with this Policy and all relevant Data Security Directives irrespective of where the Boston College data might be located, including, for example, on home devices, mobile devices, on the Internet, or other third-party service providers.

- When access to information is no longer required by a User, disposing of it in a manner to insure against unauthorized interception of any Confidential or Internal Use Only information. Generally, paper-based duplicate copies of Confidential documents should be properly shredded, and electronic data taken from Confidential databases should be destroyed.

- Immediately notifying his or her cognizant Data Security Officer of any incident that may cause a security breach or violation of this policy.

6. *Vice President for Human Resources.* The Vice President for Human Resources shall be responsible for:

- Working with the Data Security Working Group to educate incoming employees (including temporary and contract employees) regarding their obligations under this policy and to provide on-going employee training regarding data security;

- Ensuring that terminated employees no longer have access to University systems that permit access to Confidential or Internal Use Only information; and

- Carrying out any disciplinary measures against an employee taken in response to a violation of this policy as required by the Data Security Committee.

SECURITY BREACH RESPONSE

As provided above, Users and Data Security Officers must report any known Security Breach or any incident that is likely to cause a Security Breach. These incidents include thefts of computer devises, viruses, worms, or computer "attacks" that may lead to unauthorized access to confidential information.

Immediately upon becoming aware of a likely Security Breach, the Director of Computer Policy and Security shall notify the Office of the General Counsel and the Director of Internal Audit. ITS Security and Internal Audit shall conduct an investigation. The General Counsel shall determine what, if any, actions the University is required to take to comply with applicable law, including whether any notification is required under Massachusetts law. The General Counsel shall work with other administrators as appropriate to ensure that any notifications and other legally required responses are made in a timely manner. If the event involves a criminal matter, the Boston College Police Department shall be notified and shall coordinate its response with the Office of the General Counsel.

ITS Security and Internal Audit shall investigate and review the incident with the department(s) directly affected by the incident, the appropriate Data Security Officer(s). Internal Audit, in conjunction with the Director of Computer Policy and Security, shall prepare a formal report that will be distributed to the Data Security Committee and appropriate department members immediately after the investigation is finalized.

Quarterly, the Directors of Computer Policy and Security and Internal Audit will present a summary of data security investigations and/or relevant data security updates to the Data Security Committee, who shall conduct a post-incident review of events and determine, what, if any changes should be made to University practices or policies to help prevent similar incidents. The Committee shall document the University's actions in response to a Security Breach and its post-incident review in the minutes of the meeting in which the breach is discussed.

ENFORCEMENT SANCTIONS

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this policy. Violations of this policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this policy may result in dismissal from the University.

Approved: William P. Leahy, S.J.
Date: December 31, 2010rev

BOSTON COLLEGE
Data Security Policy
http://www.bc.edu/content/dam/files/offices/policies/pdf/policies/I/1-100-200.pdf

Boston College Computer System Security Requirements

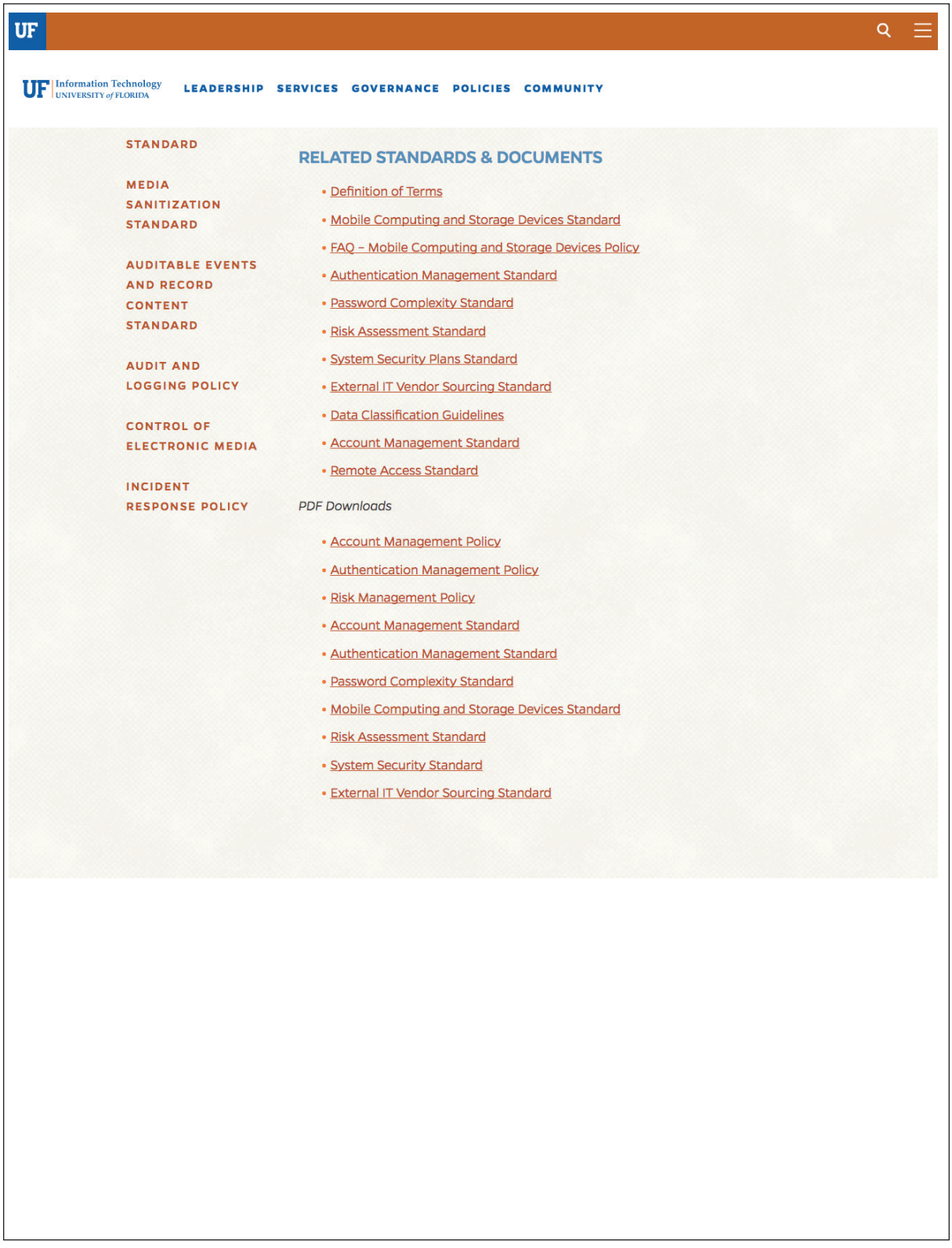
The University maintains a computer security system that provides at a minimum to the extent technically feasible:

1. Secure user authentication protocols including:
    a) control of user IDs and other identifiers;
    b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
    c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
    d) restricting access to active Users and active User accounts only; and
    e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.
2. Secure access control measures that:
    a) restrict access to records and files containing Confidential information to those who need such information to perform their job duties; and
    b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.
3. Encryption of all transmitted records and files containing Massachusetts PI that will travel across public networks, and encryption of all data containing Massachusetts PI to be transmitted wirelessly.
4. Reasonable monitoring of systems, for unauthorized use of or access to Massachusetts PI.
5. Encryption of all Massachusetts PI stored on laptops or other portable devices.
6. For files containing Massachusetts PI on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Massachusetts PI.
7. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
8. Education and training of employees on the proper use of the computer security system and the importance of data security.

UNIVERSITY OF FLORIDA
Information Security
https://it.ufl.edu/policies/information-security/#unrestricted



UNIVERSITY OF FLORIDA
Information Security
https://it.ufl.edu/policies/information-security/#unrestricted



JOHNS HOPKINS UNIVERSITY
POLICY ON ACCESS AND RETENTION
OF RESEARCH DATA AND MATERIALS

January 2, 2008

INTRODUCTION

The following policy paper contains parameters for Research Data and Materials Management (hereafter to be referred to as Research Data). In recent years, the amount of scrutiny and inquiry into Research Data has increased from a variety of sources, which has prompted efforts at Johns Hopkins and elsewhere to evaluate and update their Research Data Management practices.

The purpose of this policy is to protect researchers and the university. These measures are designed to address compliance requirements for researchers while diffusing some of the burden associated with Research Data Management. At Johns Hopkins, the department, research administration, divisional and university administration and the researcher are partners in managing and protecting the Research Data produced at the university.

This policy provides an umbrella approach to Research Data Management across the university. Divisional and other policies may also apply but are not to conflict with the overarching policy. This policy has been carefully designed to serve the best interests of our researchers and the university in management of Research Data. This policy is designed to complement, not supersede, other policies of the Johns Hopkins University including (but not limited to) protection of human subjects, HIPAA, intellectual property, financial management, etc. This policy does not apply to academic issues.

1. DEFINITIONS

RESEARCH DATA AND MATERIALS: Research Data is defined as information recorded in physical form, regardless of form or the media on which it may be recorded. For the purposes of this policy, Research Data is further defined as including any records that would be used for the reconstruction and evaluation of reported or otherwise published results. Research Data also includes materials such as unmodified biological specimens, environmental samples, and equipment. Examples of Research Data and Materials include laboratory notebooks, notes of any type, photographs, films, digital images, original biological and environmental samples, protocols, numbers, graphs, charts, numerical raw experimental results, instrumental outputs from which Research Data can be derived and other deliverables under sponsored agreements.

PRIMARY RESPONSIBLE INVESTIGATOR: The individual who bears primary responsibility for technical, programmatic, fiscal, and administrative requirements of the project.

2. APPLICABILITY OF POLICY: This Policy on Access and Retention of Research Data and Materials shall apply to all Johns Hopkins University faculty, staff, postdoctoral fellows, students and any other persons, including consultants, involved in the design, conduct or reporting of research performed at or under the auspices of the University.

JOHNS HOPKINS UNIVERSITY

Policy on Access and Retention of Research Data and Materials

http://dms.data.jhu.edu/wp-content/uploads/sites/27/2016/08/JHUDataRetentionPolicy2008_WithAppendices.pdf

3. OWNERSHIP OF RESEARCH DATA: The University owns all Research Data generated by research projects conducted at or under the auspices of the Johns Hopkins University regardless of funding source, unless specific terms of sponsorship, other agreements or University policy supersede these rights.

This policy does not attempt to determine relative rights of researchers and issues surrounding collaborative efforts such as authorship.

4. RETENTION AND ARCHIVING: The Primary Responsible Investigator of a research project is responsible for selection of an appropriate method of storing and archiving Research Data, and for determining what needs to be retained in sufficient detail and for an adequate period of time to enable appropriate responses to questions about accuracy, authenticity, primacy, and compliance with laws and regulations governing the conduct of research. The Primary Responsible Investigator is responsible for educating all participants in the research project of their obligations regarding Research Data, and for protection of the University's rights and ability to meet obligations related to the Research Data. The Primary Responsible Investigator should also consult with University officials regarding the development of any contingency plans.

5. RIGHTS TO ACCESS: The Primary Responsible Investigator will have access to the Research Data generated by the project. Any other faculty, staff, student or person involved in the creation of Research Data may have the right to review that portion of the Research Data that he or she created. The University will have access to the Research Data as necessary for technology transfer, compliance and other purposes. The University also has the option to take custody of the Research Data as determined by the appropriate University official. Such option will not be invoked without cause and subsequent notification of the Primary Responsible Investigator. In some instances, a research sponsor has a legal right of access or access may be requested through the sponsoring agency under the federal Freedom of Information Act (FOIA). Such requests will be coordinated through the Office of the General Counsel and/or the appropriate Research Administration Office.

6. DESTRUCTION OR REMOVAL: Research Data must be maintained for the periods required by law, University policy and sponsored agreement terms (See Appendix V). Thereafter, Research Data must not be destroyed without prior approval of the appropriate University official. With respect to removal of the Research Data, the University recognizes the importance of Research Data to the future research and career of its faculty. Therefore, should removal of Research Data be approved, for example, because of the transfer of the investigator to another institution, the following requirements apply:

I. Researchers may receive approval to remove original Research Data. The University may retain copies.
II. Research Data generated during the Researcher's employment at the University will be maintained in accordance with Johns Hopkins policy
III. Research Data that are integral to the ongoing research of another Johns Hopkins employee or student will continue to be made available for that purpose
IV. The researcher bears full responsibility for making original Research Data available to Johns Hopkins or federal and legal entities upon request.

Others involved in the project may remove copies (but not originals) of the Research Data with permission of the Primary Responsible Investigator.

7. MAINTENANCE AND REVISION OF THE RESEARCH DATA: The Primary Responsible Investigator of the research project is the person directly responsible for maintenance of Research Data created on that project. In order to support the project's credibility and the University's rights and ability to meet obligations related to the Research Data, should any revisions to final Research Data be contemplated, the Primary Responsible Investigator must notify the appropriate offices in the University and the originator of the information. The Primary Responsible Investigator must retain the original Research Data. See also Appendix IV.

APPENDICES, WEB LINKS, AND/OR FORMS:

I. RESPONDING TO REQUESTS FOR ACCESS BY NON-HOPKINS ENTITIES UNDER FOIA (Policy and Cost Reimbursement Form)
II. TRANSFER OF RESEARCH DATA FROM JHU CUSTODIANSHIP (Optional Approval Form)
III. LINK TO UNIVERSITY POLICIES (http://jhuresearch.jhu.edu/policies.htm)
IV. APPROVED METHODS OF ARCHIVAL
V. TIME MINIMUMS FOR ARCHIVAL

JOHNS HOPKINS UNIVERSITY

Policy on Access and Retention of Research Data and Materials

http://dms.data.jhu.edu/wp-content/uploads/sites/27/2016/08/JHUDataRetentionPolicy2008_WithAppendices.pdf

APPENDIX IV

Approved Methods of Archival for Research Data

1. Requirements for the recording and storage of Research Data and material will vary by discipline. Primary Responsible Investigators should always adhere to guidance provided by funding bodies, professional guidance where available, any principles set out on the division level as well as the University's recommendation as outlined below and in records management policies endorsed by the Chief Information Officer (CIO).

2. Research Data should be stored using a method that permits a complete retrospective audit if necessary. Unless ethical/professional/local or funding body guidance requires otherwise, Research Data should be archived in a durable form and in a secure location that is immune to subsequent tampering and falsification for a minimum period of 5 years after the date of any publication upon which it is based. It is recommended good practice that evidence for research based on clinical samples or relating to public health should be retained as required by the funding agency, federal laws, or other policies of the University.

APPENDIX V

Time Minimums for Research Data Archival

Research Data	**Laws, Policies and Regulations**	**Time Periods**
Proposals not funded	Not defined, but may contain proprietary information	Not defined
Expired Grants and Contracts	- Office of Management and Budget (OMB) Circular A-110* - Grants Policy of Funding Agency	OMB - Three years after completion of the entire research project Federal - follows OMB Private – Varies--see specific policy
Clinical Trials (All relevant records)	Food and Drug Administration (FDA) Notice: "Good Clinical Practices: Consolidated Guidelines"	At least two years after the last approval of a marketing application or at least two years after formal discontinuation of clinical development of the investigational product or longer if required by contract, but in no instance less than three years after the completion of the Clinical Trial
- Patent files - Data in support of patent	U.S. Patent Law	17 years from the date of the patent application
Research Data which supported enactment of a federal, state or local law	Not defined	Indefinite

* = OMB Circular A110 Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations"
NOTE: If a sponsored agreement exists, see specific archival requirements contained therein.

Search this site

Explore KSAS

JOHNS HOPKINS
KRIEGER SCHOOL
of ARTS & SCIENCES

The Johns Hopkins University Homewood Institutional Review Board

Home (http://homewoodirb.jhu.edu/) / Investigators (http://homewoodirb.jhu.edu/investigators/) / Data Security

Data Security

Using Personal Identifiers Security Checklist

Data Security Measures When Using Personal Identifiers

1. Avoid copying or downloading sensitive data from any administrative systems to your desktop computer, home computer, laptop, mobile device, portable storage device, etc. unless absolutely required.
2. If downloading is unavoidable:
   a. Check to see if there are unnecessary confidential data variables included in the data set, such as Social Security Numbers. If so, then delete those data variables.
   b. Ensure that if you delete private information using a "track changes" feature, that you "accept all changes" and save your document in final form, not showing your markup.
   c. When possible, use a random study ID number to identify the data from each subject, and store the code or link in a location that is physically separate from the dataset itself.
   d. Encrypt the data
   e. Password Protect the data
   f. Physically protect devices that can be easily moved such as a laptop
   g. Use remote "Kill" functionality where possible.
3. Never store your subjects' personally identifiable information on your

laptop, portable storage device, or any other device that can be lost or stolen. Instead, use a secure server.

4. Never store unencrypted data on a portable device.
5. If backing up data is required, ensure that backups are encrypted.
6. Avoid accessing personal information from computers in hotels, business centers, or any other public access locations. Remove temporary files that are created when using the internet, such as those found in browser caches and temp files.
7. If you need to use the original data collection forms and they contain personal identifiers associated with each subject, lock the originals away and use redacted copies.
8. If you store hard copies in a file cabinet or desk drawer, you must lock that storage unit. It is also preferable to be able to lock the door of the room in which the data is stored. Since several different standard file cabinets may be opened with the same key, it is advisable to get an external security bars for each of your cabinets.
9. Do not leave sensitive data unattended on a copier, printer or fax machine.
10. Dispose of documents and disks securely; use a shredder.
11. Ensure that your computer is sanitized as part of disposal.
12. Promptly report lost or stolen devices.

Title/Topic: Security of Data
Number: 6.20
Functional Classification: Information Technology
Monitoring Unit: Information Technology Services
Initially Issued: October 3, 2006
Last Revised: May 20, 2009
Last Reviewed:

SECURITY OF DATA

PURPOSE

This Policy Statement outlines the responsibilities of all *users* in supporting and upholding the security of *data* at Louisiana State University ("LSU" or the "University") regardless of *user's* affiliation or relation with the University, and irrespective of where the *data* is located, utilized, or accessed. All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of *data* from unauthorized generation, access, modification, disclosure, transmission, or destruction. Specifically, this Policy Statement establishes important guidelines and restrictions regarding any and all use of *data* at, for, or through Louisiana State University. This policy is not exhaustive of all *user* responsibilities, but is intended to outline certain specific responsibilities that each *user* acknowledges, accepts, and agrees to follow when using *data* provided at, for, by and/or through the University. Violations of this policy may lead to disciplinary action up to and including dismissal, expulsion, and/or legal action.

DEFINITIONS

For the purposes of this Policy Statement, the following definitions shall apply:

Computing resources: shall be defined as all devices (including, but not limited to, personal computers, laptops, PDAs and smart phones) owned by the University, the user or otherwise, which are part of or are used to access (1) the LSU network, peripherals, and related equipment and software; (2) *data* communications infrastructure, peripherals, and related equipment and software; (3) voice communications infrastructure, peripherals, and related equipment and software; (4) and all other associated tools, instruments, facilities, and the services that make use of any technology resources owned, operated, or controlled by the University. *Computing resources* or components thereof may be individually assigned or shared, single-user or multi-user, stand-alone or networked, and/or mobile or stationary.

Data: shall include all information that is used by or belongs to the University, or that is processed, stored, maintained, transmitted, copied on, or copied from University *computing resources*.

Data Steward(s): shall be defined as the *functional unit(s)* that is responsible for the

collection, maintenance, and integrity of the *data*.

Functional unit(s): shall include any campus, college, program, service, department, office, operating division, vendor, facility *user,* or other person, entity or defined unit of Louisiana State University that has been authorized to access or use *computing resources* or *data*.

Least privilege: shall be defined as the principle that requires each person and/or functional unit be granted the most restrictive set of privileges needed for the performance of authorized tasks.

*"***Protected information:** shall be defined as *data* that has been designated as private or confidential by law or by the University. *Protected information* includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other personally identifiable information), research *data*, trade secrets, and classified government information. *Protected information* shall not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any *data* constitutes *protected information*, the *data* in question shall be treated as *protected information* until a determination is made by the University or proper legal authority.

User(s): shall be defined as any person or entity that utilizes *computing resources,* including, but not limited to, employees (faculty, staff, and student workers), students, agents, vendors, consultants, contractors, or sub-contractors of the University.

GENERAL POLICY

Louisiana State University *functional units* operating or utilizing *computing resources* are responsible for managing and maintaining the security of the *data*, *computing resources* and *protected information*. *Functional units* are responsible for implementing appropriate managerial, operations, physical, and technical controls for access to, use of, transmission of, and disposal of *data* in compliance with this policy. This requirement is especially important for those *computing resources* that support or host critical business functions or *protected information*.

Protected information will not be disclosed except as provided by University policy and procedures, or as required by operation of law or court order.

Any electronic *data* of the University shall be classified as public, private, or confidential according to the following categories:

- Public *data* - Public *data* is defined as *data* that any person or entity either internal or external to the University can access. The disclosure, use, or destruction of public *data* should have no adverse effects on the University nor carry any liability (examples of public *data* include readily available news and information posted on the University's website).

- Private *data* - Private *data* is any *data* that derives its value from not being publicly disclosed. It includes information that the University is under legal or contractual obligation to protect. The value of private *data* to the University and/or the custodian of such *data* would be destroyed or diminished if such *data* were improperly disclosed to others. Private *data* may be copied and distributed within the University only to authorized users. Private *data* disclosed to authorized, external users must be done in accord with a Non-Disclosure Agreement (examples of private *data* include employment *data*).
- Confidential *data* - Confidential *data* is *data* that by law is not to be publicly disclosed. This designation is used for highly sensitive information whose access is restricted to authorized employees. The recipients of confidential *data* have an obligation not to reveal the contents to any individual unless that person has a valid need and authorized permission from the appropriate authority to access the *data*, and the person revealing such confidential *data* must have specific authority to do so. Confidential *data* must not be copied without authorization from the identified custodian (examples of confidential *data* include personally identifiable information in student education records, and personally identifiable non-public information about University employees).

Please see Classification of Data for a general guide to determine which data classification is appropriate for a particular information or infrastructure system.

Although some protected information, private data, and confidential data the University maintains may ultimately be determined to be "public records" subject to public disclosure, such status as public records shall not determine how the University classifies and protects data until such a determination is made. Often public records are intermingled with confidential data and protected information, so all the information and data should be protected as confidential until it is necessary to segregate any public records.

It shall be the responsibility of the *data steward(s)* to classify the *data, with input from appropriate university administrative units and legal counsel*. However, all individuals accessing *data* are responsible for the protection of the *data* at the level determined by the *data steward(s)*, or as mandated by law. Therefore, the *data steward(s)* are responsible for communicating the level of classification to individuals granted access. Any *data* not yet classified by the *data steward(s)* shall be deemed confidential. Access to *data* items may be further restricted by law, beyond the classification systems of Louisiana State University.

All *data* access must be authorized under the *principle of least privilege,* and based on minimal need. The application of this principle limits the damage that can result from accident, error, or unauthorized use. All permissions to access confidential *data* must be approved by an authorized individual, and written or electronic record of all permissions must be maintained.

Protected information shall not be provided to external parties or *users* without approval from the *data steward.* In cases where the *data steward* is not available, approval may

be obtained by the Director or Department Head of the office in which the *data* is maintained, or by an official request from a senior executive officer of the University (i.e., President, Chancellor, Executive Vice Chancellor/Provost, or Vice Chancellor).

When an individual that has been granted access changes responsibilities or leaves employment, all of their access rights should be reevaluated and any access to *protected data* outside of the scope of their new position or status should be revoked.

Data that is critical to the mission of the University shall be located, or backed up, on centralized servers maintained by the institution, unless otherwise authorized by the *data steward* of that *data,* or Office of the Vice Chancellor for Information Technology (OVCIT).

In the interest of securing information protected under FERPA, GLBA, HIPAA, other state and federal legislation, University policies (e.g. PS-113: Social Security Number Policy), and reducing the risks to the University of fines and other penalties, all users of *computing resources* shall follow Best Practices for Confidential, Private, or Sensitive Data and Best Practices for Securing Systems.

NOTE: *Please see Data Encryption for options to secure data.*

PROCEDURES

Complaints or concerns about violations of this or other technology policies should be sent to security@lsu.edu. After verification is complete using system or other logs, and in accordance with other applicable policies and procedures, the incident will be reported to the appropriate Dean, Director, or Department Head for review and possible action.

SOURCES

PS-1 Equal Opportunity
PS-06.15 Use of Electronic Mail (E-mail)
PS-06.25 Privacy of Computing Resources
PS-10 Internal and External Communications/Advertisements
PS-30 Privacy Rights of Students (Buckley Amendment)
PS-40 Employee Records Confidentiality
PS-107 Computer Users' Responsibilities
PS-113 Social Security Number Policy
PS-114 Security of Computing Resources
LSU Code of Student Conduct
PM-36 Louisiana State University System Information Security Plan
The Louisiana Database Security Breach Notification Law (Act 499)

UMassAmherst
Information Technology

Published on *UMass Amherst Information Technology* (http://www.umass.edu/it)

University of Massachusetts Amherst Information Security Policy – DRAFT [1]

February 23, 2018

I. Introduction

Institutional information, research data, and information technology (IT) resources are critical assets necessary for the University of Massachusetts Amherst ("UMass Amherst") to fulfill its missions. To maximize the preservation and protection of these assets, and to manage the risks associated with their maintenance and use, this policy establishes information security governance structure, rules, technical standards, and procedures.

By approval of UMass Amherst's Chancellor, this policy exists in conjunction with all other institutional policy.

II. Policy Statements

Information security is the responsibility of every user of institutional information, research data, and information technology resources. All users who create, access, manage, or manipulate institutional information, research data, or information technology resources must comply with this policy's administrative, technical, and physical safeguards.

A. Governance

This policy establishes campus information security governance with the creation of roles and responsibilities.

- Information Security Program Management
  - Chancellor
  - Vice Chancellor and Chief Information Officer
  - Chief Information Security Officer
  - Vice Chancellors and Deans
- Information Categorization and Management
  - Data Stewards o Steward Delegate
  - Data Administrators
  - Subject Matter Experts
  - Data Custodians
- Information Security Program Implementation
  - Vice Chancellors and Deans
  - Department Chairs, Directors, Supervisors, etc.
  - Security Liaisons
  - Chief Technology Officer
  - Service Administrator
  - Users

Additional details regarding the specific roles in these categories are in section IV.

B. Information Incident Reporting

All users must report incidents involving unauthorized access to institutional information, research data, and information technology resources to the Chief Information Security Officer. You may also report them to your local information security liaison and to the UMass Amherst IT Security Team. For more information, see: https://www.umass.edu/it/security/incident-reporting [2]

C. Institutional Information and Research Data Categorization

Institutional information and research data will be categorized in alignment with federal regulations, contractual obligations, and information risk*. Specific technical controls adhere to each category. Data Stewards are responsible for the Categorization of institutional information and research data under their purview. Data Custodians are responsible for using the appropriate security controls associated with each data category.

For more information regarding the categorization of institutional information and research data, see: https://www.umass.edu/it/security/data-categorization [3]. For more information regarding the specific technical controls that adhere to each category, see: https://www.umass.edu/it/security/controls [4].

* The standards are adapted from the Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199) available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [5].

III. To Whom This Policy Applies

This policy applies to every user (including, but not limited to, all faculty, students, staff, contractors, visiting researchers, or guests and volunteers) who accesses, manages, or manipulates institutional information, research data, or information technology resources.

IV. Responsible Parties

Every person at UMass Amherst has a responsibility to protect institutional information, research data, and information technology resources that they use or are otherwise within their control. These responsibilities vary based on the functional role of the individual. Depending on those functions, some individuals may have more than one role. This section identifies roles and their corresponding responsibilities. For more information and examples, see: https://www.umass.edu/it/security/roles [6].

A. Information Security Program Management

The following roles have responsibility for University of Massachusetts Amherst information security framework, oversight, and assistance.

1. Chancellor

The Chancellor has primary responsibility for campus information security and safety. The Chancellor may delegate authority for information security to the Vice Chancellor for Information Services and Strategy and Chief Information Officer.

2. Vice Chancellor for Information Services and Strategy and Chief Information Officer (CIO)

As a delegate of the Chancellor, the Vice Chancellor for Information Services and Strategy and Chief Information Officer, will provide executive oversight to the University of Massachusetts Amherst Information Security Program.

3. Chief Information Security Officer (CISO)

The Chief Information Security Officer is the University official with the authority to harmonize campus information security. The CISO is responsible for the development, implementation, and maintenance of a comprehensive information security program.

4. Vice Chancellors and Deans

The Vice Chancellors and Deans are responsible for program management oversight for the security of institutional information, research data, and information technology resources within their areas of purview.

B. Information Categorization and Management

As noted in Section II C, institutional information and research data will be categorized in alignment with federal regulations, contractual obligations, and information risk. Specific technical controls adhere to each category. Data Stewards are responsible for the categorization of institutional information and research data under their purview and the implementation of the specific technical controls that adhere to each category. Data Custodians are responsible for following the rules set by the Data Stewards. For more information see: https://www.umass.edu/it/security/information-management [7].

1. Data Stewards

Stewards have the highest level of responsibility for overseeing the categorization of institutional information and research data, and administering the privacy, security, and regulatory compliance of data sets under their purview (e.g., education records, human resources, and financial data). In the case of research data, in additional to acting as a Data Custodian, the Principal Investigator acts as the steward in consultation with research staff.

2. Steward Delegate

A steward may designate a delegate who will act on behalf of the steward for a portion or all the information and data under their purview. The delegate should be identified in writing to the Vice Chancellor for Information Services and Strategy and CIO as well as the Chief Information Security Officer, along with how long the delegation will be in place.

3. Data Administrators

Data Administrators are those individuals who are responsible for a particular line of business or who may have special knowledge of and responsibility for the compliance requirements for certain information or datasets. They have responsibility to inform the appropriate Steward(s) of any requirements or considerations that may influence policy, and set procedures, standards, or guidelines.

4. Subject Matter Experts

Subject Matter Experts are those individuals in roles with expertise such as risk, legal, compliance, privacy, and security who have a responsibility to inform the appropriate Steward(s) of any requirements or considerations that may influence policy, and set procedures, standards, or guidelines.

5. Data Custodians

Custodians are any individuals (employees, volunteers, etc.) who access, manage, or manipulate institutional information or research data. Custodians must follow campus policy and stewardship rules for handling of institutional information and research data.

C. Information Security Program Implementation

1. Vice Chancellors and Deans

In addition to the responsibilities of Vice Chancellors and Deans as noted in Section IV A 4 above, Vice Chancellors and Dean also have responsibility oversight for the implementation of the information security program within their areas of purview.

2. Department Chairs, Directors, Supervisors, etc.

Individuals who are responsible for a portion of the campus, such as a program, center, or line of business, shall develop, as needed, more restrictive information security controls for better management of risk to the institutional information or research data for which they are responsible. Supervisors may, at their discretion, create specific forms outlining the duties of their direct reports under this policy for review, signature, or workplace performance.

3. Security Liaisons

The unit security liaison is the person or persons designated by the unit head as the primary contact for the CISO. Their primary role is to share information security training in a manner that works for their unit, to be available for incidents, and provide effective communication between the UMass Amherst IT Security Team and the college or division they represent. For more information see: https://www.umass.edu/it/security/liaisons [8].

4. Chief Technology Officer (CTO)

For central information technology resources, the Chief Technology Officer, in coordination with the CISO, draws up technology architectural outlines, issues standards, and develops uniform templates for use by central IT and the campus community. For current technical architectural outlines, standards, and templates, see: https://www.umass.edu/it/architecture [9]. (Protected by NetID)

5. Service Administrator

A Service Administrator (e.g., application administrator, system administrator, or network administrator) is the individual with principal responsibility for the installation, configuration, and ongoing maintenance of an information technology system.

6. Users

In accordance with this policy, users must be aware of the value of information. They must protect information reasonably. Users must therefore follow the requirements for:

- Information technology resources
- Institutional information
- Research data

V. Standards

The user of every device connected to the campus network or that stores or transmits institutional information and research data is responsible for adherence to security control standards.

IT administrators either in UMass IT or in specific colleges or units may do the actual installation and configuration work, but it remains the responsibility of the user of that device to have those controls installed, configured and up to date (even if that simply means that when prompted to keep a computer on for its update, the user will comply with the prompt).

Faculty, staff, and researchers who do not have or accept IT administration support are still subject to these rules and assume all responsibility for maintaining up to date controls on their devices that store or transmit institutional information and research data. This rule applies whether it is an institutionally owned device or personal, and whether it is on the campus network while physically on the campus or from a remote location.

A. Technology Standards

All information technology resources, regardless of ownership, that contain institutional information or research data must have the following foundational information security controls in place and functioning. Alternative, but equally effective, controls may be substituted in accordance with the exception process. Additional controls may be required based on the categorization of the information or data, the nature of the information technology resource, the applicable regulatory or contractual requirements, or other risk management calculations. For more information see: https://www.umass.edu/it/security/controls [4].

1. Foundational Information Security Controls

The five foundational information security controls identified at the time of this policy's publication are referenced below. For additional information, or to see a complete, updated list of foundational information security controls, see https://www.umass.edu/it/security/controls [4]

a) Patch Management

Security patches must be installed, operational and regularly updated on all information technology resources.

b) Anti-Malware

Anti-malware solutions must be installed, operational and regularly updated for applicable information technology resources.

c) Firewall

Software to block incoming connections, unless explicitly allowed, must be installed and configured on applicable information technology resources.

d) Encryption

All institutional information and research data stored on end-user devices must be encrypted.

e) Secure Disposal

All information technology resources that contain institutional information or research data must be disposed of in an authorized manner.

B. User Account Standards

The campus owns all accounts, including NetID. IT creates and provisions these accounts to users for the purposes of accessing university resources. All users have a responsibility to protect the university accounts under their care. Protection of these accounts

may vary according to the risk that they present. Accounts with enhanced privileges may have additional requirements. For additional information including account standards, and password complexity rules, see: https://www.umass.edu/it/security/access [10].

At a minimum, all accounts must adhere to the following:

1. Credential Sharing

Credentials for individual accounts must not be shared.

2. Password Complexity

UMass Amherst IT sets password complexity requirements for your NetID. It is against policy for a user to subvert those requirements. Other password protected accounts must establish passwords with equivalent or greater complexity as the NetID requirements.

VI. Terms and Definitions

Assets: Information technology resources, such as hardware and software, institutional information, research data, and intellectual property.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Custodians: See "Institutional Information and Data Custodians" below.

Data Categorization: See "Institutional Information and Research Data Categorization".

Data Custodians: Any individuals (employees, volunteers, etc.) who access, manage, or manipulate institutional information or research data. Custodians must follow campus policy and stewardship rules for handling of institutional information and research data.

End-User: Anyone who consumes an information service. For more information see "User".

End-User Devices: Information Technology system operated by users; e.g. Desktop and Laptop computers, Mobile phones, tablets, etc.

Information security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Service: A collection of information technology systems through which a user can access, manipulate, or create campus assets.

Information Technology (IT) Resources: Anything that generates, stores, processes or transmits electronic information. This includes end-user devices and information technology systems.

Information Technology System: A subset of information technology resources that collectively provide an information service to end-user devices.

Institutional Information: Any information, regardless of medium, in the furtherance of the campus mission, excluding research data.

Institutional Information and Research Data Categorization: The exercise of mapping data to the appropriate security categories as identified in FIPS-199.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Network: A group of information technology resources and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

Research Data: All recorded information, regardless of medium, and all actual samples or examples, that were created or gathered and that could serve to influence or support a research finding or conclusion. Data does not include such items as research papers cited by

the researcher, preliminary notes or manuscripts, reviews, or related communications, or items that are already the property of others. This definition is intended to characterize current research norms, not to modify them.

Service Security Plan: Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

User: A person who accesses, manages, or manipulates institutional information, research data, or information technology resources. This definition includes, but is not limited to, all faculty, students, staff, contractors, visiting researchers, or guests and volunteers.

VII. References

1. Confidentiality of Institutional Information Technology Resources Policy
   http://www.umass.edu/it/security/conf-policy [11]
2. Acceptable Use of Information Technology Resources Policy
   http://www.umass.edu/it/security/acceptable-use-policy [12]
3. Records Retention and Disposition Schedules
   http://www.umass.edu/records/record-retention-and-disposition-schedules [13]
4. Secure Disposal of Information Technology
5. UMass Amherst IT Security Center
   http://www.umass.edu/it/security [14]

Source URL: http://www.umass.edu/it/policies/drafts

Links:
[1] http://www.umass.edu/it/policies/drafts
[2] http://www.umass.edu/it/security/incident-reporting
[3] http://www.umass.edu/it/security/data-categorization
[4] http://www.umass.edu/it/security/controls
[5] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
[6] http://www.umass.edu/it/security/roles
[7] http://www.umass.edu/it/security/information-management
[8] http://www.umass.edu/it/security/informationsecurityliaisons
[9] http://www.umass.edu/it/support/security/informationtechnologyarchitecture
[10] http://www.umass.edu/it/security/access
[11] http://www.umass.edu/it/security/conf-policy
[12] http://www.umass.edu/it/security/acceptable-use-policy
[13] http://www.umass.edu/records/record-retention-and-disposition-schedules
[14] http://www.umass.edu/it/security

UNIVERSITY OF MINNESOTA
Driven to Discover℠

University of Minnesota
https://twin-cities.umn.edu/
612-625-5000

Printed on: 08/07/2018. Please go to http://policy.umn.edu for the most current version of the Policy or related document.

UNIVERSITY OF MINNESOTA

ADMINISTRATIVE PROCEDURE

Sharing Data with University Educational and Administrative Audiences

Related Policy: Internal Access to and Sharing University Information

This procedure provides guidance on how and when members of the University community can share public or private unit record data and or aggregate-level data with audiences internal to the University. This procedure applies to all University providers of data, including individuals and units, including central units (e.g., Office of Institutional Research, central-work streams such as Human Resources, etc.), as well as colleges, departments and other units.

Individuals or units providing data in any form, including the secondary release of data, are responsible for the application of this procedure and its related policy (see Administrative Policy: *Public Access to University Information*).

The standard for sharing personally identifiable private student data is defined in the Regents Policy on Student Education Records. The policy defines "legitimate educational interest" as "an interest in reviewing student education records for the purpose of performing an appropriate University research, educational, or administrative function. The University uses the same definition of "legitimate educational interest" for sharing other private data on individuals within the University.

Definitions

Unit Record Data is considered non-aggregated data at the lowest level of detail (e.g., individual student or employee level data).

Public Data is defined by Minnesota Statutes as "data collected, created, received, maintained or disseminated by a government entity" unless classified as private by statute or federal law. For purposes of this procedure, public data are those data elements that are non-FERPA suppressed. All other data are considered private. For a list of public and private data elements see the *list of examples* provided through Administrative Policy: *Public Access to University Information*.

Providers refer to individuals responsible for providing data in any form to those audiences requesting either aggregated data or detail unit record data.

Internal audiences are defined as current University employees (non-student) who have a need to know for the purpose of performing appropriate University research, educational, or administrative function and whose work assignment reasonably requires access (see the below standard).

Out of Scope

Private data (e.g., *HIPAA*, social security numbers, *PCI DSS*) that is classified as Private-Highly Restricted as defined in Administrative Policy: *Data Security Classification* will not be shared in this manner and are out of scope for this procedure.

Those receiving requests (providers) from University of Minnesota faculty and researchers should be directed to the procedure for "Sharing Data with University Faculty and Researchers".

Those receiving requests (providers) for data from external University audiences should be directed to the procedure for "Sharing Data with Audiences External to the University".

Procedural Guidelines for Sharing Data with Internal Audiences

1. Those requesting private data need to demonstrate a "legitimate educational interest". At the discretion of the data owner or data provider and on a case by case basis; requests may require review and approval by the owner of the requested content.
2. At the discretion of the data owner or provider, requests may require follow up with the respective department head, dean's office or administrative office of those requesting data to determine appropriate use and to determine if requester's work assignment reasonably requires access.
3. Providers determine if the request is for public, private, or a combination of public and private data. For a list of public and private data elements see the appendix: *Examples of Public, Private and Confidential Information* in Administrative Policy: *Public Access to University Information*.
4. If all data being requested are classified as public, providers may share the data with internal audiences in unit record form or in aggregate form no matter the cell size (see Table 1.0 below).
5. Aggregate data that is classified as private may be shared with internal audiences assuming the requester has a business need to know to perform their job duties. (see Table 1.0 below).
6. Those who do not meet the need to know requirement should be directed to the public reports available (see Administrative Procedure: *Sharing Data with Audiences External to the University*).
7. The completion of an *Access Request Form* (ARF) will be required for those requesting access to private unit record data used for query/direct access to the Data Warehouse and other PeopleSoft sources and approved by the respective data owner.
8. When sharing the data, providers should limit the data and reporting to the scope, depth and breadth that is consistent with the requester's needs.
9. Data suppression or masking is not needed for reporting containing only public data
10. Data will be shared in a number of ways including following methods:
    a. Through the web (e.g., *www.oir.umn.edu*)
    b. Through ad hoc reporting requests
    c. Through secondary release via subsidiary reporting systems

Table 1.0 – Summarizing requirements for sharing data with audiences internal and external to the University including University faculty and researchers

		A	B	C	D
		Public Data		**Private Data**	
Audiences to Share Data with	**Item**	**Aggregate**	**Unit Record**	**Aggregate**	**Unit Record**
Internal Audiences (with need to know)	**1**	Yes	Yes	Yes	ARF
Audiences External to the University	**2**	Yes	Yes	Suppression	No
University of MN Faculty and Researchers	**3**	Yes	Yes	Case-by-case	Case-by-case

Table Descriptions:

1. 1D = Access Request Form (ARF) used by those requesting query access to data
2. 2C = Suppression should be applied with no more than one private data element per aggregate
3. 2D = Private unit record data will not be shared; however appeals can be sent to the OGC
4. 3C = Requests will be reviewed on a case-by-case basis and may require a non-disclosure agreement
5. 3D = Requests will be reviewed on a case-by-case basis and may require a non-disclosure agreement

General Notes:

1. Suppression involves applying the rule of five to summarized data through the use of percentages, ranges or masking
2. Unit Record Data refers to individual student and employee level data
3. Aggregate refers to the summarization of unit record (detail) data
4. OGC refers to the Office of the General Counsel

All questions about this procedure or how to apply it should be routed to Data Governance by sending an email to *edmr@umn.edu*.

UNIVERSITY of VIRGINIA

INFORMATION SECURITY AT UVA

INFORMATION POLICY LIBRARY

HOME / INFORMATION POLICY LIBRARY / DATA PROTECTION

Data Protection

ABOUT

Users must comply with all University policies and standards for the data to which they have been granted the ability to view, copy, generate, transmit, store, download, or otherwise acquire, access, remove, or destroy. Users must also meet any additional compliance requirements for data protection stipulated by various governmental, legal, or contractual entities.

POLICY

Data Protection of University Information (IRM-003)

STANDARDS

Electronic Data Removal

Electronically Stored Information Release

Highly Sensitive Data Protection Standard for Individual-Use Electronic Devices or Media

University Data Protection Standards (UDPS 3.0)

University Use of Highly Sensitive Data

PROCEDURES

Electronic Data Removal Procedures

Electronically Stored Information Release Procedures

Highly Sensitive Data Protection Procedures for Individual-Use Electronic Devices or Media

Procedures on the Use of Data Loss Prevent (DLP) Tools

GUIDANCE

Electronically Stored Information Release - Guidance for Authorizing Officials

Security Tools

Printer-friendly version

REPORT AN INFORMATION SECURITY INCIDENT

Please report any level of incident, no matter how small. The Information Security Office will evaluate the report and provide a full investigation.

COMPLETE REPORT FORM

UNIVERSITY of VIRGINIA

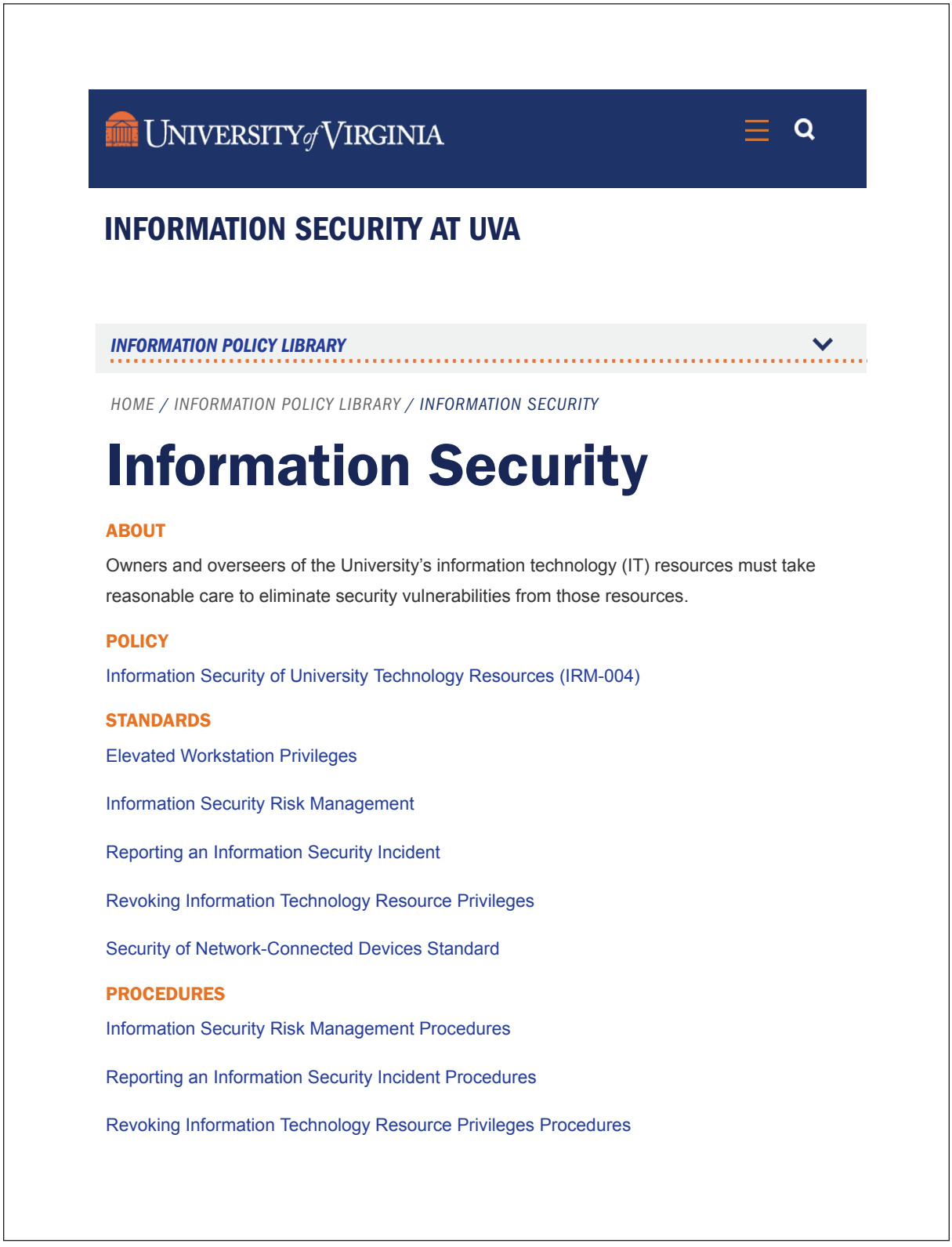
2400 Old Ivy Road
P.O. Box 400898
Charlottesville, VA 22904

EMAIL: Information Security

UVA POLICE

UVA EMERGENCY

© 2018 By the Rector and Visitors of the University of Virginia



UNIVERSITY of VIRGINIA

INFORMATION SECURITY AT UVA

INFORMATION POLICY LIBRARY

HOME / INFORMATION POLICY LIBRARY / INFORMATION SECURITY

Information Security

ABOUT

Owners and overseers of the University's information technology (IT) resources must take reasonable care to eliminate security vulnerabilities from those resources.

POLICY

Information Security of University Technology Resources (IRM-004)

STANDARDS

Elevated Workstation Privileges

Information Security Risk Management

Reporting an Information Security Incident

Revoking Information Technology Resource Privileges

Security of Network-Connected Devices Standard

PROCEDURES

Information Security Risk Management Procedures

Reporting an Information Security Incident Procedures

Revoking Information Technology Resource Privileges Procedures

GUIDANCE

Information Security Incident Response Guidelines for IT Professionals

Printer-friendly version

REPORT AN INFORMATION SECURITY INCIDENT

Please report any level of incident, no matter how small. The Information Security Office will evaluate the report and provide a full investigation.

COMPLETE REPORT FORM

UNIVERSITY of VIRGINIA

2400 Old Ivy Road
P.O. Box 400898
Charlottesville, VA 22904

EMAIL: Information Security

UVA POLICE

UVA EMERGENCY

© 2018 By the Rector and Visitors of the University of Virginia

SECRETARIAT

Guidelines for Managing Student Information for Faculties, Academic Departments and Schools

February 1, 2012

Endorsed by Graduate Operations Committee, Undergraduate Operations Committee and Deans' Council

Scope and Purpose

Student information maintained in faculties, academic departments, and schools may include information on which the admission decision was based; information regarding performance in classes and the completion of program milestones; information related to academic advising and information related to accommodation for special circumstances, petitions, discipline, grievances, and appeals. The information which the university collects, creates, and maintains about students is personal information under Ontario's Freedom of Information and Protection of Privacy Act (FIPPA).

These guidelines are a resource for faculty and staff members who manage student information. They are intended to promote awareness of the university's obligations under FIPPA, to highlight university policies and procedures relevant to student information, and to provide recommendations and best practices for managing student information.

Statutory and Policy Requirements

Faculty and staff who create or maintain student information should be familiar with the following legislation, university policies, and breach response procedure:

- *FIPPA*
- Policy 46: Information Management
- Information Security Breach Response Procedure

Responsibilities

The Registrar's Office and the Graduate Studies Office are responsible for managing the university's general, contractual relationship with undergraduate and graduate students respectively. These offices are responsible for the official student academic record maintained in the student information system (Quest).

Faculties, academic departments and schools, and associated academic support units such as Cooperative Education and the Centre for Extended Learning are responsible for managing the university's relationship with the student as a learner. They create the supporting information that documents the student's academic career including achievement in individual courses, fulfilment of program milestones and other requirements, and program completion. This information is often forwarded to the Registrar's Office or the Graduate Studies Office to authorise updates to the core student record in Quest.

Faculty associate deans, directors of schools, and chairs of academic departments are responsible for ensuring that student information created and/or maintained in their departments is kept securely and retained and disposed of according to the university's approved policies and procedures. This responsibility extends to information such as class grades, assignments, and examination papers that are often managed on a day to day basis by individual faculty members and other course instructors.

All faculty and staff are responsible for ensuring that they are managing student personal information in accordance with FIPPA and the university policies listed above. New faculty and staff members, including part-time instructors and teaching assistants, should be made aware of their responsibilities regarding privacy and retention of student information.

Privacy

The only information about a student that is considered publicly available by the university (see Policy 46) is name, degrees received and date of graduation, faculty or college of enrolment, programs of study, merit-based awards and scholarships, and directory information used to facilitate communication among students. Individual students may

request that this information not be released. See below for information about access to and disclosure of student information.

All other personally identifiable information about a student must be kept confidential according to the requirements of university policies, FIPPA, and any other legislation relevant to particular types of records. Confidential information includes:

- student ID and other identification numbers
- biographical information, such as home address and telephone number, personal e-mail address
- educational history including classes taken or enrolled in
- assessments or opinions about the student including marks and grades, comments on student work, and reference letters
- needs-based scholarships, bursaries, or awards
- photographs
- health information

Security

Student information must be kept in secure facilities and equipment (e.g., locked rooms and filing cabinets, password protected computer systems) accessible only to staff and faculty whose work requires them to have access. The university's policy with regard to information security is Policy 46: Information Management.

Extra care must be exercised if student information is taken off-campus. The use of encryption is strongly recommended to prevent or minimize the potential for a breach. See: IST's Security Standards for Desktops and Laptops, and Data Encryption pages for more information.

Keeping student information on personal equipment is discouraged. Any student information maintained on personal equipment is subject to the same security, breach response, retention, and destruction requirements as that maintained on university equipment.

Student information stored offsite or in other parts of the university must not have personal information such as names or ID numbers on the outside of the storage containers.

Security Breaches

Most student information is subject to a security classification of "restricted." Some information might be "highly restricted" (see Policy 46). Any security breach of student information (unauthorized access or disclosure, such as the loss or theft of files, laptops, or flash drives containing student information, or misdirected e-mail, etc.) must be reported immediately to the appropriate university officer (see Information Security Breach Procedure). The Information Custodian will work with the Privacy Officer who will advise whether notice to affected individuals and the Office of the Information and Privacy Commissioner of Ontario (IPC) is required. If notice is required, the Privacy Officer will provide guidance to the Information Custodian about the contents of the notice to the individuals and will laise with the IPC.

Access to Student Information

Faculty and Staff: Access to student information should be limited to faculty and staff who need the information to do their job. Information regarding accommodation for medical reasons, information related to disciplinary procedures, and needs-based financial information is considered particularly sensitive and should be accessible strictly on a need to know basis.

Students: Under FIPPA students have the right to access most personal information pertaining to them. This right extends not only to formal student files but to personal information wherever it is maintained, including in e-mail messages. The university may refuse a student access to certain types of information, for example, evaluative material received in confidence to determine suitability, eligibility, or qualifications for admission to an academic program or suitability for an honour or award.

Students do not have the right to access the personal information of individuals other than themselves. Returning assignments or exams to students or posting grades must be done in a way which does not reveal personal information to other students in the class. For more information, see Guidelines on Returning Assignments and Posting Grades.

It is also recommended that information which pertains to multiple students, such as grade revision forms, be filed separately rather than in the files of individual students.

Disclosure of Student Information

Disclosure refers to releasing student information to any party or agency (including parents, spouses, employers, and landlords) other than the student and university faculty and staff with a legitimate need to know.

Electronic posting of student personal information (including photographs) on publicly available websites (including social media sites such as Facebook) or websites available to faculty, staff, and students requires prior notice to the students who must consent to the use of their personal information in this way.

References: Be aware that information contained in references or recommendations for students is considered the personal information of the student and therefore faculty and staff members should not provide references without the consent of the student. An email from the student asking for a reference or the student naming the referee in an application can be considered consent. Students are advised to seek the agreement of potential referees before naming them in an application.

Responding to information requests

Requests from students for letters confirming their status or other academic information must be directed to the Registrar's Office or the Graduate Studies Office. Employees should be cautious about responding to requests for student information even on an informal basis. Employees may seek advice from the Registrar's Office, the Graduate Studies Office, or the university's Privacy Officer.

Retention and Disposal of Student Information

Retention: Under FIPPA the university is required to keep personal information about students for a minimum of one year.

Beyond the one year minimum, student information must be kept only as long as necessary to complete the contractual obligations between the university and the student, to provide information on the academic achievements (such as transcripts) of the student to employers, educational institutions, licensing/regulatory bodies, and to the student him/herself, and to provide the student with appropriate support and other services.

In practice, this means that different types of student information are subject to different retention periods.

The **core academic record in Quest**, which includes data on a student's identity, years of study, grades and academic milestones, and degrees and certificates earned, is the only record that the university retains indefinitely in relation to individual students.

The university's approved retention schedules for student information can be found in the **Student Management** and **Teaching & Learning** sections of WatCLASS.

Disposal: Under FIPPA, the university is also required to dispose of personal information securely and to keep a record of the disposal. Disposal must be authorized by the unit head or his/her delegate. For more information see Records Disposal Procedures.

Copies and Non-Official Information: Faculty and staff managing student information should make a clear distinction between official records and copies and other non-official information (for more information, see Managing Transitory Records).

The following are common types of non-official student information:

- Copies of forms and other documents sent to the Registrar's Office or the Graduate Studies Office
- Copies provided to members of committees
- Database extracts

- Locally maintained databases, SharePoint sites, and other electronic collections of student information

Copies and other types of non-official student information are subject to the same security and destruction requirements as official records. Non-official information should be retained only as long as necessary for current work.

Anonymous data may be preserved. If a unit wishes to keep a database (for analysis or trend purposes, for example) which is otherwise scheduled for destruction, it may do so if all identifying information of individuals is removed from it. Assistance may be sought from the university's Privacy Officer.

Electronic versus paper documents: A common misperception is that retention and disposal rules apply only to paper documents. In fact, the same rules apply regardless of the format in which the information is maintained. Therefore, when it is time to dispose of the paper copy of a document, it also time to dispose of the electronic version and vice versa.

Legal action: Student information that is related to actual or pending litigation or a government investigation must not be destroyed even if the retention period has expired. This restriction begins from the moment when a legal action or a government investigation is reasonably foreseeable, and remains in effect until removed by the Secretary of the University. Any member of faculty or staff who suspects a legal action or investigation may be pending should ensure their department head is aware of the matter. The department head should inform the Secretary of the University. The Secretary will notify you when records should be retained.

For questions or concerns regarding retention and disposal of student information, contact the University Records Manager.

E-mail

Be aware that under FIPPA a student may request to see any e-mail about him/her sent by a faculty or staff member.

Most e-mails, such as correspondence between an instructor and a student relating to a course or relating to routine inquiries, should be retained for one year and then deleted. E-mails documenting a significant decision about a student's academic career should be retained as part of the student file.

E-mail is not secure unless encrypted. Avoid use of e-mail to transmit sensitive personal or confidential information. If you must use e-mail to communicate, consider how to minimize the consequences of unintended disclosure (e.g., by disclosing only some information or by deleting personal identifiers). If you frequently use email to send sensitive information, consider whether there are other ways to deliver the information, such as use of a SharePoint site, or a secured, shared network drive. It may be better to communicate some types of information by telephone or in person.

To minimize the potential for a breach, instructors are encouraged to correspond with students only through the students' Waterloo email addresses. It is suggested that instructors indicate on course outlines that they will only respond to emails sent from students' Waterloo email addresses. See the university's Guidelines on Use of E-mail for more information.

Best Practices for Managing Student Information

- Centralize student files where possible; this ensures that all substantive records relating to a student's academic history are located in one easily accessible location, and will mean that personal information about a student can more easily be protected as well as retrieved in the case of an information access request, dispute, or some other emergency.
- When working away from campus, access student information through central systems such as Quest or OnBase or using remote desktop, rather than by removing files.
- Include information on privacy, security, retention, and disposal of student information as part of the orientation for new faculty and other course instructors, teaching assistants, and staff members.
- Make arrangements for departing course instructors such as sessional lecturers who are leaving the university and faculty members who are retiring to leave their course records (class grades, examinations and assignments, etc.) with the academic department or school.
- File students' academic information separately from employment information (e.g., records of teaching or research assistantships, co-op or work study positions). Employment information has different retention requirements than student academic information.

- File information about multiple students separately rather than in individual student files (e.g., grade revision forms, ELPE result lists). Students may access much of their own information, but must not have access to information relating to other students.
- Keep particularly sensitive information such as discipline cases or medical information separately or in the file in a sealed envelope with access restricted only to those with a legitimate need to know.
- Make copies of student information only when absolutely necessary. Copies create extra work and extra responsibility since they are subject to the same security and destruction requirements as the official record.

Securely destroy expired student information on a regular basis – once a year or once a term is usually best – following the university's records disposal procedures

Selected Resources

Books, Reports, Journal Articles, and Government Information

Asher, Andrew. "Risk, Benefits, and User Privacy: Evaluating the Ethics of Library Data." In *Protecting Patron Privacy: A LITA Guide*, edited by Bobbi Newman and Bonnie Tijerina, 43–56. Lanham, MD: Rowman & Littlefield, 2017. https://scholarworks.iu.edu/dspace/handle/2022/22035

Hagerty, John. "2017 Planning Guide for Data and Analytics." Stamford, CT: Gartner, Inc., 2016. https://www.gartner.com/binaries/content/assets/events/keywords/catalyst/catus8/2017_planning_guide_for_data_analytics.pdf

Jahnke, Lori, Andrew Asher, and Spencer D.C. Keralis. *The Problem of Data*. Washington, DC: Council on Library and Information Resources, August 2012. http://www.clir.org/pubs/reports/pub154

Jones, Kyle M. L., and Ellen LeClere. "Contextual Expectations and Emerging Informational Harms: A Primer on Academic Library Participation in Learning Analytics Initiatives." In *Applying Library Values to Emerging Technology: Decision-Making in the Age of Open Access, Maker Spaces, and the Ever-Changing Library*, edited by P. Fernandez and K. Tilton. Chicago, IL: Association of College and Research Libraries, forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2980784

Jones, Kyle M. L., and Dorothea Salo. "Learning Analytics and the Academic Library: Professional Ethics Commitments at a Crossroads." *College & Research Libraries* 79, no. 3 (April 2018): 304–23. https://doi.org/10.5860/crl.79.3.304

LAK '11. 1st International Conference on Learning Analytics and Knowledge 2011. https://tekri.athabascau.ca/analytics/

Oakleaf, Megan. "The Problems and Promise of Learning Analytics for Increasing and Demonstrating Library Value and Impact." *Information and Learning Science* 119, no.1–2 (2018): 16–24. https://doi.org/10.1108/ILS-08-2017-0080

———. "Getting Ready & Getting Started: Academic Librarian Involvement in Institutional Learning Analytics Initiatives." *The Journal of Academic Librarianship* 42, no. 4 (2016): 472–75. https://doi.org/10.1016/j.acalib.2016.05.013

Office of the Privacy Commissioner of Canada. "The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals." https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/

Office of the Privacy Commissioner of Canada. "Summary of Privacy Laws in Canada." https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Parnell, Amelia, Darlena Jones, Alexis Wesaw, and D. Christopher Brooks. "Institutions' Use of Data and Analytics for Student Success: Results from a National Landscape Analysis." National Association of Student Personnel Administrators, Inc., Association for Institutional Reseach, and EDUCAUSE, 2018. https://www.airweb.org/Resources/IRStudies/Pages/Institutions-Use-Of-Data.aspx

Rubel, Alan, and Kyle M. L. Jones. "Data Analytics in Higher Education: Key Concerns and Open Questions." *University of St. Thomas Journal of Law and Public Policy* 11, no. 1–2 (2017): 25–44. https://ir.stthomas.edu/ustjlpp/vol11/iss1/2/

———. "Student Privacy in Learning Analytics: An Information Ethics Perspective." *The Information Society* 32, no. 2 (2016): 143–59. https://doi.org/10.1080/01972243.2016.1130502

US Department of Education. "Family Educational Rights and Privacy Act (FERPA)." https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Yoose, Becky. "Balancing Privacy and Strategic Planning Needs: A Case Study in De-Identification of Patron Data." *Journal of Intellectual Freedom and Privacy* 2, no. 1 (2017): 15–22. http://doi.org/10.5860/JIFP.V2I1.6250

Consortia

Greater Western Library Alliance
Student Learning Outcomes Task Force
http://www.gwla.org/Committees/slo

Unizin
http://unizin.org/

Data Handling Policies

University of Colorado at Boulder
Data Analytics
https://www.colorado.edu/oda/

Duke University
Research Compliance Assurance
https://oarc.duke.edu/compliance/research-compliance-assurance

Emory University
Institutional Data Management
http://policies.emory.edu/10.13

Emory University
Disk Encryption Policy
http://policies.emory.edu/5.12

University of Florida
Data Management Plan
https://www.rc.ufl.edu/research/proposal-support/data-management-plan/

University of Hawai'i at Manoa
Policies and Compliance
http://www.hawaii.edu/infosec/policies/

Indiana University Bloomington
Data Management
https://datamgmt.iu.edu/index.php

Johns Hopkins University Libraries
JHU Policies for Data Management and Sharing
http://dms.data.jhu.edu/data-management-resources/plan-research/jhu-policies-for-data-management-and-sharing/

University of Michigan
Data Governance
http://cio.umich.edu/data-stewardship

New York University
Policies and Guidelines | Information Technology
https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/information-technology.html

North Carolina State University
REG 08.00.03—Data Management Procedures
https://policies.ncsu.edu/regulation/reg-08-00-03/

Pennsylvania State University
AD35 University Archives and Records Management
https://policy.psu.edu/policies/ad35

Rutgers University
Information Protection and Security
https://rusecure.rutgers.edu/policies-standards-guidance-and-compliance

Syracuse University
Information Technology Policies
https://its.syr.edu/about-us/information-technology-policies/

University of Virginia
University Information Technology Security Program
https://uvapolicy.virginia.edu/policy/IRM-011

University of Virginia
Acceptable Use of the University's Information Technology Resources
https://uvapolicy.virginia.edu/policy/IRM-002

University of Waterloo
Policy 46 – Information Management
https://uwaterloo.ca/secretariat/policies-procedures-guidelines/policy-46-information-management

University of Wisconsin–Madison
Office of Data Management & Analytics Services | Policies & Procedures
https://data.wisc.edu/policies-procedures/

Privacy Statements and Policies

University of Alabama
Privacy Statement
https://www.ua.edu/privacy/

Boston College Libraries
Privacy Statement
https://libguides.bc.edu/privacy

University of California, Irvine
Privacy and Legal Notice
https://uci.edu/privacy/

University of Delaware
General Data Protection Regulation Compliance Policy
https://sites.udel.edu/generalcounsel/policies/general-data-protection-regulation-compliance-policy/

Duke University
Office of Audit, Risk and Compliance | Privacy
https://oarc.duke.edu/privacy

Emory University
Policy 4.79. Statement of Confidentiality
http://policies.emory.edu/4.79

Emory University
Policy 8.3. Confidentiality and Release of Information About Students
http://policies.emory.edu/8.3#13

University of Florida
Privacy
http://privacy.ufl.edu/

Johns Hopkins University Libraries
Johns Hopkins Libraries Privacy and Confidentiality Policy
https://www.library.jhu.edu/policies/johns-hopkins-libraries-privacy-and-confidentiality-policy/

Louisiana State University
LSU Privacy Statement
https://sites01.lsu.edu/wp/registraroffice/privacy-guidelines/

University of Massachusetts Amherst Libraries
Responsible Use and Privacy of Library Data Statement
https://www.library.umass.edu/about-the-libraries/policies/privacy-policy/

University of Michigan Library
Library Privacy Statement
https://www.lib.umich.edu/library-administration/user-privacy-policy-university-library

University of Minnesota
Online Privacy
https://privacy.umn.edu/

University of Minnesota Libraries
Online Privacy Statement
https://www.lib.umn.edu/about/privacy

New York University
Digital Privacy Statement
https://www.nyu.edu/footer/copyright-and-fair-use/digital-privacy-statement.html

New York University Libraries
Privacy Policy
https://library.nyu.edu/privacy-policy/

North Carolina State University
RUL 02.61.02—Confidentiality of Library Records and Data
https://policies.ncsu.edu/rule/rul-02-61-02/

Oklahoma State University
Privacy Notice
https://go.okstate.edu/tos/privacy.html

University of Oregon
Student Records Privacy Policy
https://registrar.uoregon.edu/records-privacy

Rutgers University
Privacy Policy https://admissions.rutgers.edu/privacy-policy

Rutgers University Libraries
Privacy Policy
www.libraries.rutgers.edu/privacy_policy

Syracuse University
Privacy Policy
https://www.syracuse.edu/about/site/privacy-policy/

University of Tennessee
Privacy Notice
http://tennessee.edu/privacy/

Texas Tech University Libraries
TTU Libraries' Privacy Policy
http://www.depts.ttu.edu/library/about/admin/privacy_policy.php

University of Toronto
Privacy
https://www.utoronto.ca/privacy

Vanderbilt University
Privacy Policy
https://www.vanderbilt.edu/about/privacy.php

University of Virginia
Privacy Policy
http://www.virginia.edu/siteinfo/privacy

University of Virginia Library
Privacy Policy
https://www.library.virginia.edu/policies/privacy-policy/

Washington State University
Privacy Policy
https://policies.wsu.edu/privacy-policy/

Washington State University Libraries
Privacy Policy
https://libraries.wsu.edu/policies/privacy-policy

University of Waterloo
Information and Privacy
https://uwaterloo.ca/privacy/

University of Wisconsin–Madison
Website Privacy Statement
https://www.wisc.edu/privacy-statement/

Institutional Data Requests

University of Florida
Information Request Form
http://www.ir.ufl.edu/oirapps/infoir/requestform.asp

New York University
Reporting Requests
https://www.nyu.edu/employees/resources-and-services/administrative-services/institutional-research/reporting-requests.html

Western University
Policy 1.23—Guidelines on Access to Information and Protection of Privacy
https://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp123.pdf

Training

University of Florida Libraries
Research Data Management Support
http://cms.uflib.ufl.edu/datamgmt/trainings

Johns Hopkins University
Data Management Services | Training Sessions
http://dms.data.jhu.edu/training/

Library and Information Technology Association
Privacy in Libraries, a LITA webinar series
http://www.ala.org/lita/privacy-libraries-lita-webinar-series

University of Minnesota
Training and Support | FERPA resources
http://asr.umn.edu/training-and-support/ferpa-resources

Note: All URLs accessed August 16, 2018.