Institution Privacy Policies
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
COLORADO STATE UNIVERSITY
Information Collection and Personal Records Privacy
http://policylibrary.colostate.edu/policyprint.aspx?id=493

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
   1. 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
   1. 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
   1. 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
   1. e. Internal Audit Need - receives a directive from the Director of Internal Audit for information relating to specific audits or investigations; or
   1. 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
   1. 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;
   1. 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 imminent 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 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
Indiana University Policy: Privacy of Electronic Information and Information Technology Resources

IT-07

• (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
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 delegates, 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.
   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 policies and
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 to the general public, unless requested otherwise (see AD11 (polices/ad11), University Policy on Confidentiality of Student Records and HR58 (polices/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 (polices/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 PIIs 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) 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/ra02), Addressing Allegations of Research Misconduct (Formerly RA10, Handling Inquiries/Investigations Into Questions of Ethics in Research and in Other Scholarly Activities)
R07 (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:
Individually 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, 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:

<table>
<thead>
<tr>
<th>Privacy and Confidentiality Standards and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
</tr>
<tr>
<td>ESI Release</td>
</tr>
<tr>
<td>Exceptions</td>
</tr>
</tbody>
</table>

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
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
(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.