UNIVERSITY OF NOTRE DAME

Responsible Use of Data & Information Technology Resources Policy

POLICY 7.4
Responsible Executive: Chief Information Officer
Responsible Office: Office of Information Technology
Issued: September 27, 2010
Last Revised: July 2016

1. INTRODUCTION

This document constitutes the University policy for the management of its computer networks, all computers and other devices connected to those networks, and the resources made available thereby. The University of Notre Dame acquires, develops, and maintains information technology resources to support the University's instruction, research, and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas among members of the University community and between the University community and the wider local, national, and world communities.

The use of University information technology resources, like the use of any other University-provided resource and like any other University-related activity, is subject to the normal requirements of legal and ethical behavior within the University community. Responsible, acceptable use always is ethical, reflects academic honesty, is consistent with Notre Dame's mission and values, and shows community awareness in the consumption of shared resources. Occasional non-commercial personal use of Notre Dame's information technology resources is permitted (see Section 2.4 below). This Policy is intended to be an addition to existing University rules and regulations, and does not supersede or modify any other University policy, rule, or regulation.

2. POLICY STATEMENTS

When using Notre Dame's information technology resources, users must:

2.1 Comply with all federal, Indiana, and other applicable law; all generally applicable University rules and policies; and all applicable contracts and licenses. Users must use information technology resources only for lawful purposes, and not for any purpose that is illegal, immoral, unethical, dishonest, damaging to the reputation of the University, inconsistent with the mission and values of the University, or likely to subject the University to harm. Examples include but are not limited to the laws of defamation, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking," and similar activities; published University policies governing student, faculty and staff conduct, including the use of the cyber environment in violation of the University's Sexual Harassment Policy; and all applicable licenses.

2.2 Use only those information technology resources they are authorized to use, and use them only in the manner and to the extent authorized. All users of these resources must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Accounts, passwords, and access to University information technology resources may not, under any circumstances, be shared with, transferred to, or used by, persons other than those to whom they have been assigned by the University. All Notre Dame community members are responsible for their uses of University information technology resources on and off campus, and for ensuring that their systems are maintained and used so they do not endanger, impede access to, or threaten the privacy or security of others' information or systems.

2.3 Respect the finite capacity of those resources and limit use to the extent needed for authorized activities, so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. The University may require users of information technology resources to limit or refrain from specific uses in accordance with this principle. The University will judge the reasonableness of any particular use in the context of all of the relevant circumstances.

2.4 Refrain from using those resources for commercial purposes or for personal financial or other gain. The University permits occasional non-commercial personal use of Notre Dame's information technology resources. Such use should not consume a significant amount of those resources, interfere with job performance or other University responsibilities, interfere with the efficient operation of the University or its information technology resources, and must be otherwise in compliance with this Policy. The University assumes no responsibility for the loss or recovery of personal files.

2.5 Never use University resources to post, view, print, store, or send obscene, pornographic, sexually explicit, or offensive material, except for officially approved, legitimate academic or University purposes.

2.6 Comply with the law with respect to the rights of copyright owners in the use, distribution, or reproduction of copyrighted materials, including but not limited to music or video files. Unauthorized use or distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject user to civil or criminal liabilities. United States copyright law provides for a variety of potentially severe sanctions related to copyright infringement, including injunctions, impounding and disposition of infringing articles, monetary damages (either actual damages or statutory damages of up to $30,000 for each work infringed), recovery of attorneys' fees and costs, and criminal sanctions under certain circumstances. The University is also required by law to investigate claims of possible copyright infringement taking place through its computer networks. Internal University sanctions for unauthorized use or distribution of copyrighted material range from warnings to the loss of privilege to use University information technology resources.

2.7 Understand that uses of information technology resources are not completely private. The normal operation and maintenance of the University's technology resources require backup and caching of data and communications, logging of activity, monitoring of general use patterns, and other such activities that are necessary to provide service.

The University reserves the right to inspect any activities or accounts of individual users of University information technology resources, including individual login sessions and

communications, without notice, unless otherwise prohibited by law. The University may inspect such information technology resources under circumstances when the University determines inspection is necessary, including but not limited to the following:

a. To protect the integrity, security, or functionality of University or other information technology resources, or to protect the University from harm;
b. There is reasonable cause to believe that the user has violated, or is violating, any Notre Dame policy or applicable civil or criminal law; or
c. An information technology resource appears to be engaged in unusual or unusually excessive activity, as indicated by monitoring of general activity and usage patterns.

Under normal circumstances, the General Counsel and the individual's dean/director or vice president, in consultation with the Chief Information Officer, must approve in advance any individual inspection, other than that which is voluntary, required by law, or necessary to respond to emergency situations.

The University, in its discretion, may use or disclose the results of any such inspection, including the contents and records of individual communications, as it considers appropriate to University personnel, third parties, or law enforcement agencies.

2.8 Appropriate use of Electronically Stored Information. The University recognizes that there is a risk of abuse and misappropriation connected to the access to electronically stored information ("ESI"), especially when the access is by someone other than the regular steward or user of the ESI. To help guard against potential abuse or misappropriation, individuals with access to ESI must:

2.8.1. Comply with all applicable laws, all applicable University rules and policies, and all contracts and licenses. Access to ESI by those other than the normal users or stewards must be only for lawful purposes, and not for any purpose that is illegal, immoral, unethical, dishonest, damaging to the reputation of the University, inconsistent with the mission and values of the University, or likely to subject the University to harm.

2.8.2. Inform and seek collaboration with the appropriate Data Steward when accessing and using information stewarded outside of the individual's own area of responsibility. Stewards have the duty to assure data is being sought for legitimate purposes and should assist accordingly. See Appendix A for assistance identifying University Data Stewards.

2.8.3. Obtain approval of the appropriate data steward(s) before releasing University information or analysis based on University information to parties outside of the University. If unsure who the appropriate data steward is, an individual should contact the Campus Data Steward for guidance. This policy does not interfere with an employee's ability to communicate with government officials and agencies in their individual capacity or with an individual's capacity to cooperate in a government investigation.

2.8.4. When using samples sizes of three or less, take care not to share information and take all necessary precautions to protect confidentiality.

2.8.5. If information, data, or reports are provided for a specific purpose, that information, data, or report should be used for those purposes only.

2.8.6. Complete and periodically renew any certification or mandatory training courses required by the appropriate Data Steward, with oversight of the Information Governance Committee if necessary. Data Stewards are responsible for deciding, maintaining, and monitoring what certifications and training courses, if any, are required for access to and use of the data they steward. All users must certify that they have reviewed and understand this Responsible Use of Data and Information Technology Resources Policy when they are assigned a Notre Dame NetID and periodically as follows:

a) When granted access to resources designated by the Information Governance Committee as requiring acknowledgement of this policy; or

b) Every five (5) years while having access to any resources designated by the Information Governance Committee as requiring acknowledgement of this policy.

3. SCOPE

This policy applies to *all users* of University information technology resources, whether affiliated with the University or not, and to *all uses* of those resources, whether on campus or from remote locations. Additional policies may apply to specific information technology resources provided or operated by specific units of the University, or to uses within specific units. Members of the University community who use resources not owned by the University must adhere to this Responsible Use policy when conducting University business.

4. ROLES AND RESPONSIBILITIES; POLICY ENFORCEMENT

Data Steward	Data Stewards are appointed by the Information Governance Committee and will: • Assign information under their stewardship to one of three security classifications: public, internal, or sensitive based upon the information's intended use and the expected impact if disclosed; • Bear primary responsibility for decisions regarding data usage and handling for the data under their stewardship. Stewardship of Highly Sensitive data elements, as defined by the Information Security Policy, is reserved for the Information Governance Committee. • Consistent with the guidelines set forth in section 2.8 above, cooperate as appropriate with requests to access ESI within their control. • Identify and authorize Designates for acting as the Data Steward's Proxy for activities within the Data Steward's

stewardship.

Enforcement	Decisions about whether a particular use of information technology resources, or a particular access or use of ESI conform to this Policy shall be made by the Provost's Office if the use involves faculty; by the Registrar's Office if the use involves students; and by the Office of Human Resources if the use involves staff. All decisions shall be made in consultation with the Chief Information Officer to ensure consistency.
Violations	The University considers any violation of this Policy to be a significant offense and reserves the right to disconnect systems from the Notre Dame network and suspend violators' use of information technology resources and/or access to information stored or managed by the University. Violations of this Policy will subject violators to the regular disciplinary processes and procedures of the University that apply to students, faculty, and staff, and may result in loss of their computing privileges and other measures, up to and including expulsion from the University or loss of employment. Illegal acts involving University information technology resources may also subject violators to prosecution or other sanctions by local, state, or federal authorities.

5. RELATED DOCUMENTS

Policy or Document	Web Address
Academic Articles Section 2/Academic Freedom	http://facultyhandbook.nd.edu/governance/
Academic Honor Code	http://www.nd.edu/~hnrcode/docs/handbook.htm
Copyright Policies (Copyright Matters)	http://www.nd.edu/copyright/
Discriminatory Harassment Policy	http://www.nd.edu/~equity/discriminatory_harassment/
Ethical Conduct Policy	http://policy.nd.edu/policy_files/EthicalConductPolicy.pdf
Highly Sensitive Information Handling Standards	http://oit.nd.edu/policies/itstandards/infohandling.shtml
Information Security Incident Response Policy	http://policy.nd.edu/policy_files/InformationSecurityIncidentResponsePolicy.pdf
Intellectual Property Policy	http://or.nd.edu/technology-transfer/for-faculty/intellectual-property-policy/

Searches of University Property/Personal Belongings	http://hr.nd.edu/nd-faculty-staff/forms-policies/searches-of-university-property-personal-belongings/
Sexual Harassment Policy	http://www.nd.edu/~equity/sexual_harassment/Policy.shtml
Strong Password Standard	http://oit.nd.edu/policies/itstandards/strongpassword.shtml

6. CONTACTS

Subject	Office or Position	Telephone Number	Office Email
Policy Clarification & Updates	Chief Information Officer	(574) 631-9700	cio@nd.edu

APPENDIX A: DATA STEWARDS

Registrar	Chuck Hurley	Students, Courses, Grades
Enrollment	Sue Brandt (Designate: Amy Chisholm)	Undergraduate Admissions (Recruitment and Application), Financial Aid, Student Accounts, Pre-College
Provost	Chris Maziar (Designate: Tracy Biggs)	Faculty Information
Human Resources	Bob McQuade (Designate: Tammy Freeman)	Employment, Compensation, Benefits, Performance Reviews
Research	Liz Rulli (Designate: Terri Hall)	Sponsored program proposals, awards, material transfer, protocols, intellectual property
Strategic Planning Institutional Research	David Bailey	Comparative data (IPEDS, USNWR), surveys, course instructor feedback
Finance	Drew Paluf	Budget, Payroll, Procurement, Financial Reporting
Investments	Mark Krcmaric	Endowment, Investment Portfolio, Investment Partners
University Relations	Micki Kidder (Designate: Brian Dean)	Alumni, Parent and Friend information; Gifts and Giving, Campaign
General Counsel	Tim Flanagan	Contracts, Litigation, University Policies
Athletics	Heidi Uebelhor	NCAA Compliance, Recruiting, Athletics Grants-in-Aid, Sport Rosters
Facilities Design and Operation	Andrew Sama	Physical spaces