Technology Policies, Guides, and Best Practices

Responsible Use Information Technology Resources

Purpose

Dickinson College is a private institution fully committed to the ideals of academic freedom, freedom of expression and cultural diversity. This policy describes the appropriate uses of computers, networks, servers, hardware and software (“Information Technology”) at Dickinson College. In addition, it describes responsibilities of individuals and Dickinson College with respect to the confidentiality and privacy of information stored on institutional computers and servers.

Scope

This policy applies to all individuals using Dickinson College’s Information Technology. Use of the college's Information Technology constitutes the user’s agreement to abide by this policy, including consent to monitoring and inspection (as permitted and limited below). “Monitoring” refers to the observation and examination of system-wide general activity, usage patterns and performance metrics, including but not limited to, CPU loads, network traffic patterns, and volume, and attached devices. "Inspection” refers to the observation and examination of individual electronic communications, including electronic mail, mailboxes, Internet use, and the contents created or stored on any college computer, server or network-related equipment. Failure to adhere to this policy may result in the loss of e-mail and/or computing/networking privileges and discipline up to and including censure, expulsion or termination of employment in addition to any applicable civil or criminal penalties.

Individual Responsibility

Library and Information Services (“LIS”) is responsible for monitoring. It is the responsibility of all individuals in the Dickinson community to use Information Technology resources in accordance with this policy. Inappropriate behavior or malicious misuse of Information Technology resources that in any way degrades college equipment and/or services or that violates the rights of others in the community or that violates the law or college policy is strictly prohibited. Each member of the community is responsible for using only those accounts or computers for which he or she has authorization and is responsible for protecting all passwords. Individuals are urged to report unauthorized use of computers, networks, or other LIS facilities on campus by calling the LIS Help Desk or by notifying the Vice President for Library and Information Services.

Institutional Privileges

Dickinson College reserves the right to monitor and allocate Information Technology resources. To accomplish allocation of resources, the system administrators may suspend or terminate privileges of individuals without notice if malicious misuse or use inconsistent with this policy, any other relevant college policy or applicable law is detected. Privileges may also be suspended, without notice, to meet time-dependent, critical operational needs.

Because of its obligations with respect to compliance and the integrity of services provided under this policy, except as outlined below, Dickinson asserts sole ownership of all electronic communications, including electronic mail, mailboxes, files and their contents, created or stored on any college computer/network related equipment.

Nothing in the policy is intended to supersede the rights, title and interests, including copyrights, of faculty and students in their intellectual property and Dickinson College asserts no ownership or proprietary rights in such works outside the intellectual property policies of the college regardless of the presence or storage of such works on any college computer, network or network related equipment.

Similarly, the college asserts no ownership or propriety rights in the works of other college employees where such works were not created for, and are not related to, their employment.

User Logins and Passwords

Access to Information Technology resources is provided via user login and password systems. Users are personally responsible for the security of the password that they select. Viewing, copying, altering or destroying any file, or connecting to a computer on the network without explicit permission of the owner is prohibited.

Passwords should be known only to the person responsible for the account and user login. Any suspected breach of password security should be immediately reported to the LIS Help Desk.

Protecting Desktop Equipment and Files

Backups and protection of files stored on employee desktop and laptop equipment are the responsibility of the user of the equipment. Users must back up their work files on a regular basis. LIS licenses software for this purpose that may be obtained by contacting the LIS Help Desk.

Individual users are responsible for safeguarding the equipment entrusted to them by the college. This includes reasonable protection of equipment from damage and theft.

Management of Personally Owned Devices

With the approval of the relevant senior officer, the college subsidizes the purchase and operation of personally owned computing devices such as smartphones to conduct college business. Employees participating in these programs are expected to treat these devices with the same care with regard to institutional information as they would college owned devices. This obligation includes the requirements that employees employ passcodes on these devices and that they establish the ability to remotely disable these devices in the event of loss or theft.

Use of Cloud Systems and Storage

Most cloud systems and storage services do not meet Dickinson College safety and security standards and are not compliant with federal data storage laws. Please contact the Help Desk (helpdesk@dickinson.edu) for information about which systems and storage options have been approved by the college.

Confidentiality and Right to Monitor and Inspect

Users of Dickinson College information technology should understand that uses of these resources are not completely private. Under normal circumstances, the General Counsel and the relevant senior officer, 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 circumstances under which such inspections without notice may occur include, but are not limited to, the following:

1. To protect the integrity, security, or functionality of college or other information technology resources, or to protect the college or individuals in the community from harm;
2. There is reasonable cause to believe that the user has violated, or is violating, any Dickinson College policy or applicable civil or criminal law; or
3. An information technology resource appears to be engaged in unusual or unusually excessive activity that disrupts the system, as indicated by system monitoring.
4. The normal operation and maintenance of the college'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 college, 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 college personnel, third parties, or law enforcement agencies.

Personal Use

Dickinson College provides Information Technology to faculty, staff and students for use in the pursuit of legitimate academic and business pursuits for the college. Incidental personal use of Information Technology is permitted provided that such use:

- Does not affect productivity, quality or service to students and others whom we serve.
- Does not interfere with the user's job responsibilities or other obligations to the college.
- Does not create a conflict of interest or contribute to personal financial gain related to commercial activity.
- Does not directly or indirectly interfere with the college's operation of electronic mail services, computing capacity or network capacity.
- Does not interfere with other users' access to or use of the campus network.
- Does not violate federal, state or local laws, or college policy.

Legal Compliance

All existing federal, state and local laws and relevant college regulations and policies apply to the use of computing resources and all users of such resources are required to be in compliance with all such laws, regulations and policies at all times. This includes not only those laws and regulations that are specific to computers and networks, but also those that apply generally to personal conduct. As such, any of these resources may be subject to review by designated college personnel in accordance with college policies.

Inappropriate Uses – Examples

The following are examples of violations of this Acceptable Use of Information Technology Resources Policy. This list is not dispositive.

- **Malicious misuse.** Using logins or passwords assigned to others; disrupting the network; destroying information; intentionally erasing stored information or modifying equipment, accounts, disks or files that are not your own; removing software from public computers; spreading viruses; sending e-mail that threatens or harasses other people; downloading, uploading or sharing images or information that violates any law; invading the privacy of others; subscribing others to mailing lists or providing the e-mail addresses of others to bulk mailers without their consent; running a personal business, downloading material from the Internet that violates federal, state or local law, or college policy (except when disclosed in advance to the Provost and Dean of the College, and determined to be related to legitimate research or learning purposes); illegally duplicating or otherwise copying copyrighted or licensed software or using illegal copies of copyrighted materials; or using Information Technology in violating any federal, state or local law.
- **Unacceptable use of software and hardware.** Knowingly or carelessly running or installing unlicensed software on any computer or computer system or network; giving another user a program intended to damage the systems or network; violating terms of applicable software licensing agreements, including copying or reproducing any licensed software; or violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, music or other materials; using imaging equipment to duplicate, alter and subsequently reproduce official documents.
- **Inappropriate access.** Unauthorized use of a computer account; providing misleading information in order to obtain access to computing facilities; using the campus network to gain unauthorized access to any computer system; connecting unauthorized equipment to the campus network including wireless access points; unauthorized attempts to circumvent data protection schemes to uncover security loopholes (including creating and/or running programs that are designed to exploit security vulnerabilities and/or decrypt intentionally secure data); intentionally locking another user out of that user's account; knowingly or carelessly performing an act that will interfere with the normal operation of computers, peripherals, or networks; or deliberately wasting or overloading computer resources.
- **Inappropriate use of electronic mail and Internet access.** Initiating or propagating electronic chain messages; inappropriate mass mailing including multiple mailings to newsgroups, mailing lists, or individuals, forging the identity of a user or machine in an electronic communication; using another person's e-mail account or identity to send e-mail messages; attempting to monitor or tamper with another user's electronic communications; reading, copying, changing or deleting another user's files or software without the explicit agreement of the owner; using e- mail or personal web page advertising to solicit or proselytize others for commercial ventures, religious or political causes, or for personal gain related to commercial activity; any use that otherwise violates federal, state or local law, or college policy.

Noncompliance and Sanctions

LIS may suspend or terminate all computing privileges of any individual without notice who engages in any improper computing activities. Serious cases, as determined by the Vice President for Library and Information Services, and in consultation with the appropriate senior officer of the division with supervisory authority over the individual may result in disciplinary action against the individual up to and including the suspension, expulsion, or termination of employment of the offending individual, as appropriate. Disciplinary actions involving faculty will be initiated in compliance with the processes outlined in the Academic Handbook. Disciplinary actions involving College administrators or staff will be initiated in compliance with the applicable personnel procedures. Disciplinary actions involving students will be referred to the student disciplinary hearing process by the Dean of Students or his/her designee or the Provost and Dean of the College or his/her designee. Where violation of federal, state or local law is involved, cases and related information may be referred to the proper legal authorities for action.

Revised April 24, 2016

Technology Overview
Technology Services
Teaching With Technology
Technology Policies

Technology Policies

- **Responsible Use Information Technology Resources**

Digital Millennium Copyright Act
Wireless Internet Access
Student Virus
Spam
Campus Cable TV Programming
College Sponsored Guest
Social Media Guide
Social Media Best Practices
Web Philosophy and Governance
Academic Software Requests
InCommon Federation Practices