Tufts Technology Services
169 Holland Street, Suite 211
Somerville, MA 02144

Use of Information Systems Policy

Purpose

This policy sets forth the manner in which Tufts' *institutional systems* are to be used in general, and particularly, when collecting, creating, using, sharing, disseminating, storing, retaining, and disposing of *institutional data*.

This policy is part of a suite of information policies that includes:

- The Information Stewardship Policy, which presents the core principles for the stewardship of *institutional data* and *institutional systems;*
- The Information Classification and Handling Policy for *institutional data*;
- The Information Roles and Responsibilities Policy, which defines the roles and responsibilities for individuals with respect to *institutional data* and *institutional systems*;
- The Network Use Policy; and
- Additional University policies, standards, guidelines, procedures, and student, faculty, and employee handbooks, including those that address specific technologies and compliance requirements.

Scope

This policy applies to all students, faculty, staff, guests, and other persons associated with the Tufts community, regardless of affiliation.

Definitions

Institutional Data. All information that is created, discovered, collected, licensed, maintained, recorded, used, or managed by the University, its employees, and agents working on its behalf, regardless of ownership or origin. Such information is *institutional data* regardless of the ownership of any device, machine or equipment used to create, discover, collect, store, access, display, or transmit the information.

Institutional Systems. The electronic and physical systems owned, leased, licensed, managed, or otherwise provided by Tufts University used to create, discover, collect, store, access, display, or transmit *institutional data*. *Institutional systems* include, without limitation, desktop computers, laptops, servers, printers, scanners, copiers, research equipment, telephone systems, email systems, networks, databases, and cloud storage services, other software applications and services, and other devices, machines, equipment, and hardware. *Institutional systems*, such as software applications, that have been loaded onto a device, machine or other equipment that is not owned, leased, licensed or otherwise provided by Tufts, continue to be subject to the provisions of this policy.

Policy Statement

The University's *institutional systems* support the University's mission, including all University-related activities. Each user of these *institutional systems*, like those of other University resources and activities, is responsible for using the systems in accordance with all applicable laws and regulations; University policies, procedures, guidelines, standards, and student, faculty and employee handbooks; and University licenses and other contracts. All use of *institutional systems*

must be consistent with Tufts' values and mission and University expectations for ethical behavior.

Responsibility to Protect Access Provided to Institutional Systems

Tufts *institutional systems* are provided to authorized individuals for University-related purposes. All access and use must be properly controlled in a manner defined by management, and consistent with individual roles and job responsibilities. Authorized access to *institutional systems* is generally expected to end when a user no longer has an official connection to the Tufts community.

Persons associated with the Tufts community are entrusted with access to *institutional systems* on an individual basis. Users are not permitted to extend access further to any other person by any means, including sharing access by providing a password or by other means, providing unauthorized redistribution of services or data, or otherwise obfuscating or misrepresenting the true identity of the user.

Users are expected to take reasonable steps to prevent unauthorized access and use. These steps include, but are not limited to, information security controls, such as the configuration of hardware and software, the use of anti-virus software, firewalls, and encryption; and assisting with remediation in the event of a detected or suspected vulnerability or compromise. Users are also required to comply with all University procedures, guidelines, standards, and handbooks that reduce the risk that malicious software could affect the confidentiality, availability, or integrity of *institutional data*, and that protect *institutional data* by establishing handling and other requirements.

Individuals may not attempt to gain unauthorized access to *institutional systems*, whether through hacking, password mining, or any other means, or interfere or attempt to interfere with the proper working of *institutional systems*.

Limitations on the Personal Use of Institutional Systems

All users of *institutional systems* are expected to respect the priority of University business and keep the personal use of *institutional systems* to a minimum. University users may use *institutional systems* for incidental personal purposes if such use does not:

i. directly or indirectly interfere with the University's operation of *institutional systems*,
ii. interfere with the user's employment or other responsibilities and obligations to the University,
iii. burden the University with noticeable incremental costs or otherwise, or
iv. involve activities for commercial gain.

Use of *institutional systems* to access or use *institutional data* for a personal purpose is prohibited.

Notwithstanding the statement of permitted uses above,

i. managers have the discretion and authority to limit or prohibit the personal use of *institutional systems*, and
ii. any such use must also comply with all applicable laws and regulations, University policies, procedures, guidelines, standards, and student, faculty and employee handbooks, and University licenses and other contracts, and must be consistent with Tufts' values and mission and University expectations for ethical behavior.

Responsibility to Not Engage in Prohibited or Restricted Activities

Whenever individuals use the University's *institutional systems*, they are required to comply with the laws and regulations and the University policies, procedures, guidelines, standards, and student, faculty, and employee handbooks that apply to the information accessed, stored, used, transmitted, or displayed using these systems. These requirements include, but are not limited to, laws, regulations, and policies that apply to:

i. Political or commercial activities affecting the non-profit, tax exempt status of the University (including as discussed below)
ii. Use of copyrighted information
iii. Use of the University's names, insignias, and other trademarks
iv. Libel, slander, and defamation
v. Harassment, including sexual or sex and/or gender based harassment
vi. Actions involving child pornography and/or obscene material

Restrictions on Political Activities. As a nonprofit, tax exempt 501(c)(3) organization, Tufts University is prohibited by federal law from participating in, or intervening in (including the publishing or distributing of statements), any political campaign on behalf of (or in opposition to) any candidate for public office. Individuals may not use University resources for political purposes in a manner that suggests the University itself is participating in campaign activity, fundraising, or other political or commercial activities. This policy does not prohibit use of University resources to discuss or examine political topics or issues of public interest, so long as it does not involve advocacy for or against a particular candidate and the use is consistent with the University's Policy on Political Activities. Registered student organizations may use University resources for political activities when the use is consistent with the University's Policy on Political Activities.

Responsibility to Comply with Local and System Policies and Practices

The University employs various administrative, technical, and physical controls to reduce inherent risks associated with using *institutional systems* and to safeguard *institutional data*. However, security cannot be guaranteed solely with centralized controls. School, division, departmental, and individual controls, policies, and practices should establish and maintain appropriate access control and security, such as anti-virus software, firewalls, and secure storage areas for physical media; management of user accounts, proper authentication and verification of identity, including two-factor authentication; and authorized forms of encryption for *institutional data* and *institutional systems*.

Users must comply with the policies, guidelines, and standards for each specific set of *institutional systems* they access and with the policies, guidelines, or standards established by schools, divisions and departments. When the policies, guidelines, or standards established by the University, or by a school, division, or department, or for a specific *system*, are more restrictive than those established by this policy, then the more restrictive provisions will take precedence.

Responsibility to not Interfere with Management Controls for Institutional Systems

Administrative, physical, and technical controls serve to reinforce Tufts' interpretations of responsible use, verify trust placed in individuals, and limit their authorization to *institutional systems* and *institutional data*. Disabling, removing, damaging, circumventing, or interfering with such controls threatens the entire network of *institutional systems*, and is a violation of this policy. Anyone who seeks to or gains unauthorized access to an *institutional system* or *institutional data* is in violation of this policy.

Under management direction, the University performs testing and audits of its security controls to help ensure they are working as intended. Users are prohibited from probing or testing security controls of any *institutional system*, unless such actions have been expressly approved in writing by an authorized employee responsible for the security of such system or such actions are expressly included among the security evaluation responsibilities of the employee's position.

When an *institutional system* has been, or is suspected of having been, compromised or may not be operating under appropriate management control - and in order to protect the confidentiality, integrity, or availability of *institutional systems*, *institutional data* or to otherwise protect the University - management may disable, disconnect, or contain any account, device or system, prior to, during, or upon completion of an investigation.

Responsibility to Avoid Resource Exhaustion and Disrupting Use by Others

Operation of *institutional systems* must respect the finite capacity of those systems and limit use so as not to consume an unreasonable amount of systems capacity or to interfere unreasonably with the activity of other users. The University may require users of *institutional systems* to limit, schedule, coordinate, or refrain from specific uses in order to ensure that adequate resources are available to all users.

University Administration of System Use

The University places a high value on privacy and recognizes its critical importance in an academic setting. While Tufts does not routinely monitor individual usage of resources, normal operation and maintenance of resources requires logging of activity, backup and caching of data, and other activities necessary to provide services and ensure adherence to laws and regulations and University policies.

In accordance with state and federal law, the University may, at its sole discretion and without notice to the individual:

i. Access any University *institutional system* activity (including viewing the contents and records of any individual communication) of individuals without notice whenever there is reasonable cause to believe that a law, regulation, contract, or any Tufts policy is being or has been violated, or that such actions are needed to protect the health or safety of the individual or other persons;
ii. Utilize the results of any general or individual monitoring, including the contents and records of individual communications, in appropriate University disciplinary proceedings or in litigation or other legal proceedings;
iii. Disclose the results of any such monitoring, including the contents and records of individual communications, to appropriate University personnel; local, state, or federal law enforcement or administrative agencies; or pursuant to legal process (such as a subpoena); and
iv. After the employment of an individual who was either faculty or staff ends, access such individual's University *institutional system* activity (including the contents and records of any individual communication) if there is a legitimate University business reason.

Policy Violation

Depending on the circumstances, and in management's sole discretion, persons who violate University policies may be denied access to *institutional data* and *systems*, and may be subject to other penalties and disciplinary action, both within and outside of the University. The University may refer suspected violations of applicable law to appropriate law enforcement agencies.

Review Entities

Risk and Compliance Committee
IT Steering Committee
Information Stewardship Subcommittee

Approval Date

September 15, 2011; revision December 3, 2012; revision June 6, 2018

Effective Date

September 20, 2011; revision December 3, 2012; revision June 6, 2018

Executive Sponsor

Tufts Technology Services, Office of the Chief Information Officer

Policy Managers

Tufts Technology Services
Digital Collections and Archives
University Counsel

Responsible Offices

For general questions about the policy

- Tufts Technology Services
- Digital Collections and Archives
- University Counsel

For questions about using electronic *institutional systems*, contact Tufts Technology Services.

Revision

The University reserves the right to change this policy from time to time. Proposed changes will normally be developed by the policy managers with appropriate stakeholders. The review entities have sole authority to approve changes to this policy.

Distribution

Related Policies

Information Stewardship Policy
Information Roles and Responsibilities Policy
Information Classification and Handling Policy
Network Use Policy
Policy on Political Activities
Email Policy
Mailing List Policy
Policy on the Use of Tufts University Names and Insignia
Tufts University Policy on the Fair Use of Copyrighted Materials
Non-Discrimination Policy
Sexual Misconduct Policy