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

Information Roles and Responsibilities Policy

Purpose

This policy establishes the roles and responsibilities that all, faculty, staff, guests, and other persons associated with the Tufts community have for the appropriate management, use, and stewardship of *institutional data* at Tufts University.

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 Use of Information Systems Policy, sets forth the manner in which Tufts' *institutional systems* are to be used; and
- Additional University policies, procedures, guidelines, standards, and student, faculty, and employee handbooks, including those that address specific technologies and compliance requirements.

Scope

This policy applies to all faculty, students, 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

Responsibilities

Faculty, students, staff, and other persons associated with the Tufts community manage and use *institutional data* to support their work. Using and managing *institutional data* comes with a variety of responsibilities, including those described below.

All management and use of *institutional data* should represent Tufts' values and mission and management expectations for ethical behavior.

All faculty, students, staff, and other persons associated with the University community are obligated to:

- *Protect the Confidentiality of Institutional Data* as provided in the Information Stewardship Policy, the Business Conduct Policy and other applicable University policies.

- *Respect Individual Privacy* by protecting the privacy of personal information as provided in the Information Stewardship Policy, the Business Conduct Policy and other applicable University policies. Respecting the privacy of personal information includes not placing *institutional data* on *institutional systems* or other environments that are unfit or unauthorized for such purposes, or engaging in activities that unnecessarily expose *institutional data* to harm or unauthorized access.

- *Comply* with all applicable laws and regulations; University policies, procedures, and standards; and licenses and other contracts in their management and use of *institutional data*. All faculty, students, staff, and other persons associated with the Tufts community are responsible for using and managing *institutional data* in a compliant manner. All faculty, students, staff, and other persons associated with the University community who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those other states and countries and the rules and policies of external networks and systems. Users should ensure that their use of any particular resource is consistent with laws within those other jurisdictions.

- *Respect for Copyright and Intellectual Property of the University, Members of the Tufts Community and Others as provided* in the Policy on Fair Use of Copyrighted Materials and the Policy on Rights and Responsibilities with Respect to Intellectual Property.

Effect of University 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.

Roles

Members of the Tufts community play different roles in the governance, use and management of *institutional data*. These roles and the associated responsibilities are described below. An individual may have different roles for different types of *institutional data*. This policy is designed to help members of the community understand their responsibilities and others' responsibilities in the interconnected framework for governing, using, and managing *institutional data*.

Provost and Executive Vice President. The role of each of the Provost and the Executive Vice President includes the following with respect to *institutional data:*

- Provides leadership for the University's data strategy and vision

- Provides policy direction and oversight regarding the governance, use and management of *institutional data*
- When needed, resolves issues and questions relating to data access, use and management that may arise for Data Authorities, Data Authority Delegates, persons requesting access to and use of *institutional* data, and others.

Academic Council (AC). This council's role includes the following with respect to *institutional data:*

- Advises on the University's data strategy and vision
- Provides policy direction regarding the governance, use and management of *institutional data*
- Reviews and approves policies pertaining to *institutional data* in accordance with the University's governance process for policy approvals

Data Owners. Generally speaking, Tufts University is the information owner of *institutional data*. Faculty members are often information owners of their faculty materials. See the Policy on Rights and Responsibilities with Respect to Intellectual Property for more details on ownership rights.

IT Steering Committee. This committee's role includes recommending university-wide IT policy and strategy, including data governance.

Information Stewardship Subcommittee (ISS). The ISS is a subcommittee of the IT Steering Committee.

- A core role of the ISS is to initiate and contribute to developing university-wide policy and strategy for the stewardship of *institutional data*. This responsibility includes developing and recommending new policies, as well as regularly evaluating, reviewing, and recommending revisions to existing policies, for information management and stewardship. Considerations include information security, privacy, government and industry regulation, and information management principles, with an objective of maximizing *institutional data's* value in support of the university's vision and mission.
- The ISS works closely with and acts as a coordinating body for the Data Authorities and Data Authority Delegates. Through its work with the Data Authorities and the Data Authority Delegates, the ISS supports the development and implementation of appropriate and consistent policies, procedures, requirements, and guidelines for the stewardship of *institutional data,* including the approval and removal of access to *institutional data,* and the collection, storage, use and safekeeping of *institutional data*, whether across the University, within or across data types, or within data classifications. The ISS or its chairs, may, from time to time, as needed, provide for a meeting of the Data Authorities and/or Data Authority Delegates, with or without members of the ISS, to facilitate the work of the Data Authorities and the Data Authority Delegates.
- The ISS is co-chaired by the Director of Information Security, TTS, and the Associate Provost responsible for education and student affairs. Its members include representatives from administrative and school offices and departments across the University and faculty.

Data Authorities. Each Data Authority is assigned to and has primary responsibility for a particular data type or domain. Each data type or domain generally has one Data Authority. A Data Authority:

- Ensures the data is assigned a confidential classification under the Information Classification and Handling Policy
- Identifies the federal, state, and other applicable laws and regulations; University

policies, procedures, guidelines, and standards; and applicable licenses and other contracts that affect the data under their care
- Identifies authorized users of the data, whether by individual identification or by job title or role
- Develops and approves policies, guidelines, standards, and procedures specific to the particular data type or domain, defining specific access, handling, use, and management requirements
- Provides communications and education to information users on the appropriate use and care of the data
- Interprets and applies policies, guidelines, standards, and procedures for the particular data type or domain
- Coordinates with, advises, and oversees their Data Authority Delegate(s)
- Works with Information Technology Administrators to establish and maintain trustworthy information systems for the particular data type or domain
- Coordinates their work with the ISS
- Participates in meetings and deliberations of the Data Authorities

Data Authority Delegates. Each Data Authority may designate one or more Data Authority Delegates to whom they may delegate authority to make determinations about the data type or domain. Each Data Authority Delegate is assigned to and has primary responsibility for a particular data type or domain. Each data type or domain may have more than one Data Authority Delegate, who coordinate their work for a particular data type or domain. Data Authority Delegates process data access and use requests and apply policies, guidelines, standards, and procedures for the assigned data type or domain. They provide communications and education to information users on the appropriate use and care of the data. Data Authority Delegates may exercise some discretion in their application of policies, standards, and procedures to particular requests, based on guidance from the Data Authority. Data Authority Delegates are responsible to and report to the applicable Data Authority for their work as a Data Authority Delegate. Data Authority Delegates are required to document their determinations for all data requests. The Delegates will also work with Information Technology Administrators to establish and maintain trustworthy information systems for the particular data type or domain. Data Authority Delegates coordinate their work with the ISS and participate in meetings and deliberations of the Data Authority Delegates.

Information Technology Administrators follow and implement the decisions granting or disabling access to *institutional data* as made by the Data Authorities and the Data Authority Delegates and follow and implement all applicable policies, guidelines, standards, and procedures with respect to managing the *institutional data*. The Information Technology Administrators will work with the Data Authorities and the Data Authority Delegates to establish and maintain trustworthy information systems for the particular data type or domain, including by maintaining and operating *institutional systems* in a manner commensurate with the confidentiality level of the institutional data held or accessed by the *institutional systems*. The Information Technology Administrators also work with managers to meet requirements for working with *institutional data*. The Information Technology Administrators generally are Tufts Technology Services staff.

Managers of University units, departments, and offices are responsible for the proper management and protection of *institutional data* by their unit, department, or office.

Information Stewards in each of the University's departments and offices are responsible for organizing and supporting the proper handling in their department or office of sensitive information through the Information Steward Program. Information Stewards carry out their

responsibilities by coordinating and collaborating with their group's manager. The roles and responsibilities of an Information Steward include those set forth in the written plan for the Massachusetts Data Privacy Program with respect to personal information. The Information Steward Program's initial focus on Sensitive Personal Information (SPI) will expand over time to include other sensitive information. A steward's responsibilities include:

- Being knowledgeable about best practices for protecting the sensitive information
- Understanding how their department or office uses the sensitive information
- Evaluating and developing their department or office's policies and practices to protect the sensitive information
- Coordinating and supporting implementation of university and local policies and procedures to safeguard handling of the sensitive information
- Raising the awareness of the staff, faculty, students, and others that are part of their department or office of the importance of protecting the sensitive information and acting as a resource as staff and others implement practices to protect the sensitive information.

Information Users include all members of the University community. Information Users are responsible to comply with, and are guided by, all laws, regulations, Tufts policies, guidelines, standards, procedures, agreements, contracts and licenses that apply to the *institutional data* they use.

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

IT Steering Committee
Information Stewardship Subcommittee

Approval Date

September 15, 2011; revision June 6, 2018

Effective Date

September 20, 2011; 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

Tufts Technology Services

Digital Collections and Archives
University Counsel

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
Use of Information Systems Policy
Information Classification and Handling Policy
Business Conduct Policy