



Integrated Information Technology Services

POLICIES AND PROCEDURES

Responsible Use of University Computing Resources

POLICY:

As part of its educational mission, Utica University acquires and maintains fixed and mobile computers, computer systems, mobile phones, smartphone devices, and related networks (collectively referred to as “computing resources”). These computing resources are intended to be used for University-related purposes, including direct and indirect support of University instruction, research, and service; University operations and 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 local, regional, national, and global communities.

The rights, responsibilities, and limitations of academic freedom apply to the use of University computing resources. The use of University computing resources, like the use of any other University-provided assets, property, or services, is subject to the requirements and standards of legal and ethical behavior, as they evolve over time, within the University community. Legitimate use of a computer, computer system, phone device, or network does not extend to whatever is technically possible. Limitations built into computer operating systems and networks are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

All users of University computing resources must:

- Comply with all federal, state, and other applicable laws, all applicable University rules and policies, and all applicable contracts and licenses between the University and academic partners or the University and vendors relating to University computing resources. Such laws, rules, and policies include, but are not limited to, libel, defamation, privacy, copyright, trademark, obscenity, and child pornography laws; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit hacking and similar activities; the Digital Millennium Copyright Act governing, among other things, digital rights management and certain copyright infringement within and outside the United States; the Higher Education Opportunity Act, which mandates that higher education institutions develop and implement a written plan to effectively combat unauthorized distribution of copyrighted materials by users of the institution’s network; the College’s student and employee handbooks; and the University [Copyright and Peer-to-Peer File-Sharing](#), [Sexual Harassment](#), [Gender-Based Harassment](#), and [Sexual Misconduct](#), and [Employee Code of Conduct](#) policies. Users who engage in electronic communications with persons in other states or countries or on other systems or networks

should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks, and may be exposed to viruses and other network-disrupting software or programs. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

- Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not *per se* imply authorization to do so, nor does it imply that IITS will support the resource. Users are responsible for determining which authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the University. For more information, see the University's [Computer Passwords](#) and [Purchasing and Accounts Payable](#) policies.
- Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for determining which authorizations are necessary and for obtaining them before proceeding.
- Limit bandwidth use so as not to consume an unreasonable amount of resources or to interfere unreasonably with the activity of other users, particularly instructional use. The University may choose to limit or restrict specific uses, as determined by Integrated Information Technology Services (IITS), taking into account relevant facts and circumstances. For more information, see the University's [Vulnerability and Risk Assessment](#) policy.
- Refrain from using computing resources for personal commercial purposes or for personal financial or other gain. For more information, see the University's [Employee Code of Conduct](#) policy.
- Refrain from storing personal files on work machines or network drives, or using their University issued email account for personal use. Further limits upon personal use may be imposed by IITS in consultation with an employee's supervisor.
- Refrain from using University-owned computers to view pornographic materials unless permission is granted for academic purposes.

Vendor Acceptable Use:

In addition to the above rules, each vendor may have its own policies on acceptable use. Violating those terms may result in the termination of accounts with or without prior notification to the user, system administrator, or University personnel. It is the responsibility of all users to familiarize themselves with the requirements for each vendor with which they interact. In most cases, vendor acceptable use terms and policies can be found online or by contacting the vendor directly.

SCOPE:

This policy applies to all users of University computing resources, whether affiliated with the University or not, and to all uses of those resources, whether on University property or from remote locations.

This policy also applies to all forms of social media, such as Facebook pages, Twitter accounts, web pages, and other sites created or accessed by University users.

REASON FOR POLICY:

This policy is designed to protect the safety and individual rights of Utica University students and employees, comply with federal and state laws, safeguard the University from legal action, and provide an environment where the University network is safe and reliable.

DEFINITIONS:

Public: Data that must be controlled from creation to destruction. Applies to information that has been approved by Utica University for release to the public. Access is typically available and may be kept in

unlocked storage devices or publicly available websites. When the data is no longer needed on a regular basis, it should be archived or disposed of. Guidance for records retention and destruction can be found in the [Records Retention](#) policy.

Private: Information that must be guarded against unauthorized generation, access, modification, disclosure, transmission, or destruction due to its proprietary, ethical, or privacy considerations. Any information not created specifically for public distribution should be considered private unless otherwise classified with a more restrictive classification.

Examples of applicable laws and regulations include:

- Protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA)
- Student educational records as defined by Family Educational Rights and Privacy Act (FERPA) and the Gramm Leach Bliley Act (GLBA)
- Cardholder data as defined by the Payment Card Industry (PCI) Data Security Standard

Examples of private data include:

- Academic records
- Health records
- University partnerships
- Social Security numbers
- System passwords
- Financial information

Sensitive: This data is highly confidential and may contain research, law enforcement, governmental, or other data. Only those directly involved with these processes are to have access to this information.

PROCEDURE:

Many procedures for complying with this policy are outlined in the policy statement above. In addition:

The University employs various measures to protect the security of computing resources, data, and users' accounts. Users should be aware, however, that the University cannot guarantee such security. Users should therefore engage in prudent computing practices by establishing robust access restrictions for their accounts. This includes guarding their passwords and changing them regularly. For more information, see the University's [Computer Passwords](#) policy.

The University and its employees are responsible for protecting private and sensitive University data. Should any University computing resources become compromised or threatened due to loss or theft of information technology equipment or other resources, users must immediately take steps to prevent or minimize the harm or damage that could result. If a University-owned device or personal device containing Utica University data or used to access Utica University data is lost or stolen, users must immediately notify the Office of Campus Safety and IITS. Should this occur off-campus, users should file a police report with appropriate local authorities. IITS will contact the user after the reported loss or theft to determine the nature and scope of any compromised Utica University private or sensitive data, and may take steps to delete data from these devices. If there was a potential compromise of private or sensitive information or exposure of network resources, the Director of Information Security may confer with appropriate University officials, coordinate notification to affected individuals, and report the incident to state or federal agencies as required. For more information, see the both the College's [Data Breach Notification](#), and Data Security and Classification policies.

Users should also be aware that their use of University computing resources is not private. Part of the normal operations of the University's computing resources require monitoring of general and specific usage, data capacity, general and specific activity. In certain situations, the University may also monitor the activity and accounts of individual users of University computing resources, including individual

login sessions and communications, without notice. Examples of those situations may include, but are not limited to the following situations:

- The user has given permission or has voluntarily made them accessible to the public, for example by posting to a publicly accessible web page or providing publicly accessible network services.
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of the University or other University-related computing resources, including network or internet traffic, or to protect the University from liability or reputational harm.
- There is a reasonable basis to believe that the user has violated, or is violating, this policy or other technology-related policies.
- An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
- The University is conducting audits as defined by the [Vulnerability and Risk Assessment](#) policy.
- It is otherwise required or permitted by law.

Any such individual monitoring, other than the specified in paragraph (a) above, that is required by law or necessary to respond to perceived emergency situations, must be authorized in advance by the Vice President of Legal Affairs and General Counsel.

Users who violate this policy may be denied access to University computing resources and may be subject to other penalties and disciplinary action, both within and outside the University. Violations will normally be handled through the University disciplinary procedures applicable to the relevant user. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, through the disciplinary system administered by the Office of Student Affairs. The University may temporarily suspend, throttle, or block access to computing resources prior to the initiation or completion of such procedures when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University computing resources or to protect the University from liability or reputational harm. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings. Communications made by means of University computing resources, including the contents and records of individual communications, may also be subject to review as part of private lawsuits and proceedings to the same extent as they would be if made on paper.

RESPONSIBILITY:

It is the responsibility of IITS to investigate any suspected or reported violations of this policy. It is the responsibility of University employees who witness breaches of this policy to report violations to IITS.

ENFORCEMENT:

Enforcement of Utica University policies is the responsibility of the office or offices listed in the “Resources/Questions” section of each policy. The responsible office will contact the appropriate authority regarding faculty or staff members, students, vendors, or visitors who violate policies.

Utica University acknowledges that University policies may not anticipate every possible issue that may arise. The University therefore reserves the right to make reasonable and relevant decisions regarding the enforcement of this policy. All such decisions must be approved by an officer of the University (i.e. President, Provost and Senior Vice President for Academic Affairs, Vice President for Financial Affairs, Senior Vice President for Student Life and Enrollment Management, or Vice President for Legal Affairs and General Counsel).

RESOURCES/QUESTIONS:

For more information, contact the Director of Information Security. Use of University computing resources is also subject to the University's Code of Student Conduct, the College's policy on Academic Misconduct, and all other generally applicable University policies including:

[Computer Passwords Policy](#)

[Copyright and Peer-to-Peer File Sharing Policy](#)

[Data Breach Notification Policy](#)

Data Security and Classification Policy

[Employee Code of Conduct](#)

[Purchasing and Accounts Payable Policy](#)

User Accounts Policy

[Utica University Email Policy](#)

[Vulnerability and Risk Assessment Policy](#)

Please note that other Utica University policies may apply or be related to this policy. To search for related policies, use the Keyword Search function of the online policy manual.

Laura M. Casamento, President

Date

Effective Date: April 1, 2013
Promulgated: April 12, 2013

Last Revised: March 9, 2019
Promulgated: