Westfield State University
Policy concerning:

Section: Administrative
Number: 0380
Page: 1 of 7

APPROVED: March 2000

REVIEWED: February 2025

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

PURPOSE

The purpose of this policy is to provide guidelines for the appropriate use of information technology resources at Westfield State University (“University”) and establish sanctions for violations of this policy. This policy is intended to protect the users of the University’s information technology resources by ensuring a reliable and secure technology environment that supports the educational mission of the University. These resources are provided as a benefit to all Westfield State University employees, students, and authorized guests. The University seeks to ensure the integrity of information technology resources made available to the community and to prevent disruption to academic and administrative needs. This policy is not intended to inhibit the culture of intellectual inquiry, discourse, and academic freedom.

In general, the same ethical conduct that applies to the use of all University resources and facilities applies to the use of the University’s information technology resources.

SCOPE

This policy applies to all students, faculty, and staff of the University, and to all other users who are authorized by the University to access its information technology resources. This policy is supplemented by the policies of those networks to which the University is interconnected, including, but not limited to, the University of Massachusetts Information Technology Systems group, the Commonwealth of Massachusetts’ Information Technology Division, UMass Online, etc.

For the purposes of this policy, “Information Technology Resources” means all computer and communication facilities, services, data, and equipment that are owned, managed, maintained, leased, or otherwise provided by the University.

USER OWNERSHIP AND RESPONSIBILITIES

It is the responsibility of any person using the University’s information technology resources to read, understand, and follow this policy. In addition, all users are expected to exercise reasonable judgment in interpreting this policy, and in making decisions about the use of information technology resources. Any person with questions regarding the application or meaning of this policy should seek clarification from his or her supervisor, or from the Office of Information and Instructional Technology.

The University owns and maintains the information stored in its information technology resources, and it limits access to its information technology resources to authorized users. Users of information technology resources have a responsibility to properly use and protect these resources, respect the rights of other users, and behave in a manner consistent with any local, state, and federal laws and regulations, as well as all University policies. Information technology resources, including Internet bandwidth, are shared among the community, and users must utilize these resources with this understanding.

Users must respect all intellectual property rights, including any licensing agreements applicable to information and resources made available by the University to its community.

Information technology resources are provided to support the mission of teaching and learning and to conduct official University business. Therefore, the University bears no responsibility for the loss of any personal data or files stored or located on any system.

The University does not systematically monitor communications or files. Users must be aware of, or responsible for, material which community members may post, send, or publish using its network, servers, and other resources including the Web.

UNACCEPTABLE USES OF UNIVERSITY INFORMATION TECHNOLOGY RESOURCES

The University permits limited, occasional, or incidental personal use of its information technology resources. Even when occasional usage is permitted, faculty, staff, students, and other authorized users should use discretion when using information technology resources for personal reasons.

The University prohibits the use of its information technology resources for the following purposes:

- in furtherance of any illegal act, including the violation of any criminal or civil laws or regulations, whether local, state, or federal.
- for any political purpose.
- for any commercial purpose.
- to violate any University policy.
- to discriminate against any person on the basis of any legally protected characteristic.
- to harass any person based on any legally protected characteristic, including sex.
- to access or share sexually explicit, obscene, or otherwise inappropriate materials.
- to infringe any intellectual property rights.
- to gain, or attempt to gain, unauthorized access to any computer or network.
- for any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs.
- to intercept communications intended for other persons.
- to misrepresent either the University or a person's role at the University.
- to libel or otherwise defame any person.
- to use e-mail or messaging services to threaten, harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted e-mail, or by using someone else's name or user-id.
- to waste computing, network, or technology resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters, unsolicited mass mailings or crypto mining.
- to add, remove or modify equipment comprising the Information technology resources at the University unless they have been explicitly authorized to make such changes by the Chief Information Officer or his representative.

- to install on the University’s network for any purpose or use any peer-to-peer file sharing applications. In addition, any other network-based, non-academic application that consumes the University’s bandwidth may be limited or restricted. The Chief Information Officer must approve the installation of any server or server-based application on the University’s network.

This list is illustrative and not exhaustive, and the University reserves the right to determine other prohibited activities and/or unauthorized uses that are not specifically identified in this policy.

DATA CONFIDENTIALITY

While performing their jobs, University employees and contractors often have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees or contractors to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may employees or contractors disseminate any confidential Information that they have rightful access to unless such dissemination is required by their jobs. Users of the University’s information technology resources have a responsibility to protect the confidentiality of the information to which they have access.

Personnel must adhere to the information classification system and ensure that appropriate measures are taken to protect information commensurate with its value to the institution. The information classifications include Confidential, Sensitive, and Public (see *Data Classification Policy*). The confidentiality and integrity of information must be protected at rest, in use and in transit. Protection requirements also include information governed by compliance standards requiring additional information protection requirements that may not be specifically addressed in this policy.

The following are guidelines to safeguard confidential information at rest:

- Store all information on access-restricted and/or -controlled Shared Folders or Drives (e.g., local network drives, One Drive).
- Encrypt or password-protect removable media that contain confidential information such as USB drives and mobile devices.
- Dispose of confidential information only after confirming compliance with records retention laws.

The following are guidelines to safeguard confidential information in use:

- For access to systems that host confidential information, personnel must request access using an approved access request process/tool and be positively authenticated.
- Use the minimum amount of confidential information (e.g., Social Security numbers) to the minimum necessary to support business operations (e.g., the last four digits). Store the information in approved information repositories.

- Where possible, do not store confidential information on laptops or desktops. Confidential information must be stored in Shared Folders, Shared Drives, or other secure institution systems.

The following are guidelines to safeguard Information in transit.

- Use institution-issued encryption solutions to protect the integrity of confidential information that will be transmitted outside of the institution. This can be achieved by the following:
- Use secure mail feature of email client by adding encryption the email when necessary.
- Password-protect files that contain confidential information.
- Use the institution-approved secure transfer solution for larger transfers.

COPYRIGHT PROTECTION

Computer programs are valuable intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a web site. As such, it is important that users respect the rights of intellectual property owners. Users should exercise care and judgment when copying or distributing computer programs or Information that could reasonably be expected to be copyrighted.

NETWORK SECURITY

In compliance with state and federal data security laws, the University seeks to protect the security of its information technology resources and of users' accounts, and to prevent unauthorized access by others, both on and off campus.

It is critically important that users take particular care to avoid compromising the security of the network. Most importantly, users should never share their passwords with anyone else and should promptly notify University personnel if they suspect their passwords have been compromised. In addition, users who will be leaving their PCs unattended for extended periods should log off the network.

ACCESS MANAGEMENT

The institutions must ensure that personnel are positively authenticated and authorized prior to receiving access to institution information resources. Access to systems shall be based on the user's role and must be limited to the minimum rights necessary to perform their job function. Access to information assets must be controlled through a defined process, which includes a periodic review of information system access (see *Access Management Guideline*)

1. All access must be requested on a role based need to know to perform the specific job function of the individual and their responsibilities in the department.

2. Supervisors will approve the applicable access forms (e.g. Banner Access, Network Access Request Form) and/or obtain all required signatures, physically and/or electronically.
3. Reviews of user's access to applications and/or technology infrastructure will be performed by supervisors at least bi-annually to ensure access is appropriate to perform their job responsibilities.
4. Segregation of duties: Users must not be granted access to information assets that would allow entitlements to perform job responsibilities that are not compatible with each other (e.g., having the ability to both request and approve a change).
5. The university reserves the right to make unannounced changes to the infrastructure or accessibility of any information technology resource.

SECURITY EDUCATION TRAINING AND AWARENESS (SETA)

Security Awareness is focused on the entire service population and is universally applicable to all echelons of the organization. Security awareness is an individual responsibility for all Westfield State University constituents and focuses individual attention on security needs or concerns and promotes positive security consciousness and facilitates proactive changes in security related behavior or reinforces good security practices.

Pursuant with the Commonwealths Executive Office of Technology Services and Security (EOTSS) standards personnel are required to participate in SETA programs, in the required time frame, as provided by the university to produce relevant security skills and competencies to support job performance and meet compliance requirements. *(see SETA Guidelines)*

SETA shall consist of:

- Within 30 days of hire/contract, all constituents shall be required to complete security education training and awareness.
- At a minimum, annual security education training and awareness must be completed by all constituents. Other specialized areas may require more frequent training based upon regulatory requirements or other factors necessitating more frequent training.
- At a minimum, monthly phishing tests will be sent to assess the university's security posture.

SECURE WORKSPACE

Personnel must keep their assigned workspace secure (e.g., lock confidential information in drawers, use cable locks if issued by the institution).

All personnel must be mindful of using mobile devices (e.g., smartphones and tablets) with access to institution information. Mobile devices must be secured with a password that meets or exceeds the access control requirements, where applicable, and must not be left unattended.

Employees are responsible for protecting the devices and any confidential files from theft or security breaches. Any breaches of computer security or theft should be reported immediately to Public Safety and the Chief Information Security Officer.

When personnel are telecommuting or working remotely, institution-owned devices must not be left unattended in public spaces (e.g., public transportation, restaurant, coffee shop, airport, airplane, or in a doctor's office).

Documents containing confidential information should be sent utilizing a secure print solution (e.g., Papercut) for printing. Documents that are sent to a shared printer that has direct print capability must be retrieved immediately to reduce the risk of unauthorized access.

E-MAIL

In Massachusetts, e-mail is considered a public record and must be treated as such. E-mail is subject to production pursuant to a public record request, and it is subject to the Commonwealth's record retention policies in the same manner as paper records.

When using e-mail, there are several points users should consider. First, because e-mail addresses identify the organization that sent the message (first.last@westfield.ma.edu), users should consider e-mail messages to be the equivalent of letters sent on official letterhead. Finally, although many users regard e-mail as being like a telephone in offering a quick, informal way to communicate, users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, users should not write anything in an e-mail message that they would not feel just as comfortable putting into a memorandum. (see E-mail policy).

PRIVACY/CONFIDENTALITY

The University is the owner of all information technology resources, including e-mail. As such, no student, faculty member, staff member or other authorized user has a reasonable expectation of privacy in their e-mail or any other use of the University's information technology resources.

To that end, the University cannot guarantee privacy or confidentiality in the use of its information technology resources. Under certain circumstances, the University may be legally obligated to disclose information in response to court orders or other legal actions, in response to public record requests, in disciplinary processes, in health and safety emergencies, or when necessary to protect the integrity or security of its information technology resources. The University retains full discretion in reviewing and disclosing records to comply with these requirements.

Certain classes of data are also protected from disclosure by law or regulation. In compliance with those laws and regulations, the University seeks to protect any personally identifiable information managed on its information technology resources. All members of the University community with access to such data are required to maintain the confidentiality of such data in accordance with this policy.

Information technology resources at the University are the property of the University and the Commonwealth of Massachusetts. As such, the University retains, and when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, the right to inspect any user's computer, any data contained in it, and any data sent or received by it. Any use of the University's information technology resources constitutes express consent for the University to monitor and/or inspect any data that users create or receive, any messages they send or receive, and any web sites that they access, in accordance with the requirements of the law and any relevant collective bargaining agreement.

ENFORCEMENT

Any behavior or activity that alters the normal functioning of the University's information technology resources, or which negatively impacts their use by any other member of the community, is strictly prohibited. The University retains the right to take any reasonable action necessary to protect the integrity and security of its information technology resources, to curtail illegal use of the resources, to ensure the resources are equitably shared, and to protect the rights and privacy of its users.

Users of information technology resources who violate this policy, gain unauthorized access, or violate any state, local or federal law will have their access to use information technology revoked and may be subject to the University's disciplinary processes and procedures. Violations of this policy may also result in disciplinary action, up to and including termination, expulsion, and/or legal action. Illegal acts may also subject users to prosecution by law enforcement authorities.

The use of the University's information technology resources constitutes an understanding of an agreement to abide by this policy.

REVIEW

This policy shall be reviewed annually by the Chief Information Officer.