Acceptable Use Policy

Widener University

Approved By: Eric Behrens, Vice President of Library and Information Services
Issue Date: October 2018
Revision Date(s): No revisions

Related Policies or Procedures: Information Security and Compliance Program (ISCP)
Additional References:
Responsible Officer: Widener University Chief Information Officer (CIO)

Policy:

This document constitutes a University-wide policy for the use and management of computer data networks, network resources, and computers that are owned and administered by Widener University. The policy reflects the general principles of the university community and indicates the privileges and responsibilities for the university computing environment.

Responsibilities of the User

Access to an electronic mail account, the Internet, computing resources and campus networks is a privilege to which all university faculty, staff and students are entitled. The University will make these resources available with the fewest interruptions possible. Access may also be granted to other individuals for purposes consistent with the mission of the University. Certain responsibilities accompany this privilege. These responsibilities are outlined in this document.

Security

The security of information is a shared responsibility. Widener University will assist users of its computing resources in protecting information from accidental loss, tampering, or unauthorized access. The University will take appropriate measures to ensure security and the Information Technology Services (ITS) staff will make appropriate information on security procedures available to all users. Users should be aware, however, that unauthorized users may gain access to electronic communications and files. Users who are concerned about security are encouraged to use appropriate encryption or access restrictions. Users who are concerned about verifying their identity are encouraged to use digital signatures. Additional information on encryption and digital signatures is available from ITS. System administrators of departmental and individual computing resources are responsible for the security of information stored on those resources, for making appropriate information on security procedures available to users of those systems and for keeping those systems free from unauthorized access.

As part of this responsibility, users should be certain to:

- Use passwords that are not easily broken or guessed.
- Keep passwords confidential and do not share them.
- For employee-owned or student owned systems, regularly update systems to ensure that security patches are current.
- Regularly update virus/malware protection software.
- Take necessary precautions to maintain the security of their systems and their accounts.

Confidentiality

Widener University intends that all files and email are private and confidential to the owner unless the owner intentionally makes this information available to other groups or individuals. Users may give others access to their files by making them publicly available. Users should be aware that if they make a file publicly available, anyone with the appropriate privileges will have access to the file. Widener University will assume that computer users wish information they store on central and shared computing resources to remain confidential and will maintain confidentiality of all information stored on University computing resources. Privileged information available to system administrators will be held in confidence. Interception of network transmissions (outside of official investigations by the University) is strictly forbidden.

Widener University maintains logs of network activities that include web page addresses visited from computers on and off campus. These logs are only used to manage the network traffic and are not to be used to infringe upon the privacy of network users. Private information contained in network records will not be used to compromise any user's privacy.

Users should be aware that Widener University cannot guarantee security of email. As a result, users should use discretion with email. If the privacy of a message is important, it should be encrypted, or otherwise safeguarded. Ultimate responsibility for email security rests with the user.

To protect the University community from email viruses/malware and other threats to the network, messages that meet specific criteria that indicate the presence of a threat may be intercepted. Due to the volume of email that Widener receives, users cannot be notified when a message to them has been intercepted and not delivered. Intercepted messages will not be opened without the permission of the recipient.

The University regularly backs up material on network servers. Information is preserved for a finite time and may be used to recover lost or corrupted data. Users should be aware that these backup tapes contain a record of all files, including email and network logs, on the system at the time of the backup. No guarantees are provided that information lost or destroyed can be retrieved in total.

Requests for disclosure of confidential information will only be honored when required by University Policy or by local, state or federal law.

Usage

Computer resources, network access and bandwidth may not be used for:

- Intentional harassment of others.
- Intentional destruction of or damage to equipment, software, or data.
- Intentional disruption or unauthorized monitoring of electronic communications.
- Unauthorized acquisition of and/or distribution of copyrighted and/or licensed material.
- Violations of computer system security.

- Use of computer accounts, access codes, or network identification numbers assigned to others.
- Intentional use of computer communications facilities and resources to impede the computing services available to others.
- Violation of software license agreements.
- Violation of network usage policies and regulations.
- Violation of others' right to privacy.
- Illegal purposes
- Use of computing facilities for private business purposes unrelated to the mission of the university or university life.
- Intentional use of computer communications facilities and resources in ways that unnecessarily impede the computing services available to others (e.g., randomly initiating interactive electronic communications or email exchanges, overuse of interactive network utilities, etc.).

Academic Freedom

Free expression of ideas is central to the academic process. Widener system administrators will not remove any information from individual accounts unless required by University policy or by local, state or federal law. Likewise, Widener system administrators will not block or filter any Internet content unless required by University policy or by local, state or federal law.

Purpose

The purpose of the policy is to ensure the safety and security of critical data for Widener University and to preserve the integrity of the mission of the University.

Those Affected/Scope

This policy affects all users in the Widener University community.

Compliance

Measurement

As part of the policy review process, this policy will be reviewed during any changes, and upon request.

Exceptions

As with any urgent or emergency situation, this policy can be amended or suspended upon direction from the University Executive Team.

Non-Compliance

Widener University treats the abuse of computing facilities, equipment, software, data, networks, or privileges as a risk to the University. If a user's actions present an immediate threat to the security of the network, the University may suspend access with notification until the threat is resolved. Unauthorized access to electronic communications and files is strictly forbidden. Use of computing resources is to be conducted in keeping with the guidelines established by University policy. This includes relevant sections of the Faculty and Student Handbooks, the Academic Integrity Statement, and the Freedom to Learn Policy, as required. Judicial proceedings that are adjudicated by Widener University will be resolved in the manner stated in the appropriate handbooks and policies applicable to the status of the user. Illegal acts involving Widener University computing resources may also be subject to prosecution under local, state and federal laws.

Related Policies, Standards, Regulations, and Procedures

- Information Security and Compliance Program

Effective

This policy is effective once reviewed and approved by the ISCC and the Executive Team of Widener University.

Definitions and Terms