XAVIER UNIVERSITY POLICY ON ACCEPTABLE USE OF UNIVERSITY COMPUTERS AND NETWORK SYSTEMS

CONTENTS

OVERVIEW

This policy (hereafter the "Terms") establishes rules and strategies for acceptable use of Xavier University's information technologies and resources, including all computer devices, data, applications, and the supporting networking infrastructure owned, leased, and/or managed by the University. The policy is based on the following underlying principles:

- Information resources are provided to support the essential mission of Xavier, including its teaching, scholarship, and service missions; administrative functions; student activities; and more.
- Xavier policies, state and federal law, and other regulations govern the use of information resources.
- The information resources infrastructure is provided for the entire Xavier community. This infrastructure is finite, and all users are expected to use it responsibly and ethically.
- Some actions that are technically feasible may be illegal and/or inappropriate.

Access to Xavier's networks and information technology environment is a privilege granted by the University and must be treated as such by all users of these systems. Effective security is a team effort involving the participation and support of every Xavier employee, student and affiliate who deals with information systems. It is the responsibility of every computer user to read and understand the Terms and to conduct their activities accordingly. The Terms are in place to protect the Xavier community. Inappropriate use exposes Xavier to risks including virus attacks, compromise of network systems and services, and legal issues.

Individual departments and/or administrative units may have additional, supplemental policies regarding computer equipment, networks and electronic communications. Individual policies do not supersede, replace or invalidate this policy.

STATEMENT ON ACADEMIC FREEDOM

Information resources at Xavier help to facilitate the free exchange of ideas among members of the University community and the wider community. As an academic institution, all of us at Xavier place great value on freedom of thought and expression. The University community encompasses a wide array of opinions, views, approaches, and temperaments.

AUDIENCE

The Terms apply to all individuals that have access to Xavier's information resources, including but not limited to: all faculty, staff, students, alumni, retirees, temporary workers, library patrons, visitors, contractors and vendors using University information resources, whether on- or off-site (hereafter collectively referred to as "Users").

USER RIGHTS & RESPONSIBILITIES

Members of the Xavier community are granted access to information technology resources in order to facilitate their University-related activities, including, without limitation, academic activities, service activities, student development, research, and work. Examples of acceptable uses are:

- Coursework and course management;
- Thesis preparation and research projects;
- Independent research and self-teaching projects;
- Communication with students, faculty, and staff at Xavier or at other academic institutions;
- Communication within and outside the University for purposes related to the business of the University.

Users must comply with all federal, state, and other applicable laws; all applicable University rules and policies; and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

The following examples, though not covering every situation, specify some of the rights and responsibilities that accompany computer use at Xavier and/or on Xavier's networks:

1. Using limited resources responsibly and efficiently

Users may not knowingly or intentionally engage in activities that could negatively impact the functionality of Xavier's computer systems, enterprise and application systems, and network services. Users may only use Xavier's computing resources in the manner and to the extent authorized. Users are expected to promote efficient use of network resources, consistent with Xavier's instructional, research, public service, and administrative goals. Xavier may require Users to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances. Examples of activities that violate these Terms include, without limitation, the following:

- Tampering with any hardware, networks, applications, system files or other users' files without authorization or permission; or

- Circumventing or altering software, physical protections or other restrictions placed on computers, networks, software, applications or files, including University-installed virus protection software.
- Using unauthorized filesharing applications or illegally downloading or sharing files, including, without limitation, movies, music, applications, and other software;
- Using excessive amounts of storage or creating excessive network traffic;
- Launching attacks or probes, or otherwise attempting to subvert the security of any system or network;
- Introducing, creating, or propagating any malicious programs, including, without limitation, viruses, worms, trojans, spyware, or other malicious code;
- Allowing unauthorized access to the Xavier network through any computer or network device (including wireless access points);
- Establishing or maintaining a server without prior written authorization;
- Abusing printing privileges; and
- Physically damaging systems or not returning borrowed equipment in a timely manner.

If employees or departments are considering any major hardware or software purchase, they should first contact the Information Resources Division's Office of Projects and Programs to ensure efficiency and compatibility with existing systems.

2. Privacy and confidentiality

Users are prohibited from using University technology to infringe on others' privacy. Unauthorized reading, copying, or modification of files or email is prohibited. Users may not reveal confidential information obtained from administrative data systems to unauthorized people or groups.

For more information about the privacy and confidentiality of email and data, see the separate Policy on the Privacy of Electronic Information.

3. Electronic Communication (Email, voicemail, Internet communications)

All members of the University community are encouraged to use electronic communications for University-related activities. However, those who use University communication services (email, voicemail, Internet communications via chat or social networks such as Twitter, Facebook, etc.) are expected to use them in an ethical and responsible manner.

Electronic communications should meet the same standards for distribution or display as tangible documents. Users should identify themselves clearly and accurately in all electronic communications, and never conceal or misrepresent their name or affiliation.

Users may not send obscene, pornographic, rude, or harassing messages of any kind. Users are prohibited from sending frivolous or excessive messages, including chain letters, junk mail, spam, and other types of broadcast messages. Users should exercise extreme caution when opening email attachments from unknown senders.

Xavier recommends that Users who send confidential or sensitive information electronically should encrypt and/or password-protect the documents. For information on restricting documents through password-protection or encryption, please call the Information Resources Center.

4. Information security

Users are responsible and accountable for the security of the electronic resources they own or use, including but not limited to computer account(s), passwords, personal computer(s), electronic data, and network access.

Users must use only their own computer account(s), and may not assume another person's identity or role without proper authorization. Users may not communicate or act under the name or email address of another person or entity without proper authorization.

Passwords should not be shared, even with family members or friends. Users may not supply false or misleading data or improperly obtain another's password in order to gain access to computers, network systems, data, or information, and may not attempt to subvert the restrictions associated with computer accounts or network access. Without regard to whether information on any resource (such as email, voicemail, or document files) is access-restricted, Users may not access any information on any resource maintained by or licensed to another User without proper authorization.

5. Physical security

Users are responsible to prevent others from obtaining physical access to their computer(s) and to ensure that both electronic and paper files in their care are safeguarded, especially if they contain sensitive data about individual students, employees, or others. Specific recommendations to maintain physical security include the following:

- Log off or lock workstation when leaving one's desk.
- Back up data regularly.
- Destroy drives, CDs, and other electronic media when they are no longer usable.
- Lock flash drives, CDs, and other electronic media in a desk or in a fire-resistant cabinet.
- Take special care to secure small portable devices (such as laptops and PDAs), which can be easily lost or stolen.

6. Installation of software

Users are responsible for using software and electronic materials in accordance with copyright and licensing restrictions and applicable University policies. Users may not use Xavier University networks, equipment, or software to violate copyright or the terms of any license agreement.

Most software available for use at Xavier is protected by federal copyright laws, and it is the policy of the University to respect the copyright protections given to software owners. The software provided through the University for use by faculty, staff, and students may be used on computing equipment only as specified in the various software licenses. Licenses sometimes specify that Users may use the software only while they are members of the Xavier community.

It is against University policy for faculty, staff, or students to copy or reproduce any licensed software except as expressly permitted by the software license. Installation or distribution of "pirated" or unlicensed software is prohibited and illegal.

Any software installed by Users must be consistent in intent and practice with the Acceptable Uses outlined above.

7. ***Intellectual property***

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors, inventors, trademark owners, and publishers in all media. It encompasses respect for the right to acknowledgment, rights of privacy and publicity, and right to determine the form, manner, and terms of publication and distribution of one's work.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer and network environments.

Copyright laws protect audio and video recordings, photographs, electronic books, and written material. Users sharing any content of this kind that they did not create may be infringing on another's copyright.

Violations of intellectual property rights, including, without limitation, plagiarism, unauthorized access, and trademark, servicemark, copyright, and trade secret infringement, may result in disciplinary actions by the University.

All copyrighted information that is stored, transmitted or maintained using Xavier's equipment or networks must be used in conformance with applicable copyright and other laws. The University will not protect individuals who use or share, knowingly or not, copyrighted materials without an appropriate license or permission to do so. Click here for more information about Xavier's copyright policies.

The logo, name and graphics of Xavier or Xavier's affiliates are trademarks of Xavier or its affiliates. Use, reproduction, copying or redistribution of Xavier's trademarks, without the written permission of Xavier or its affiliates, is prohibited. All other trademarks or servicemarks appearing on the Website are the marks of their respective owners. Users who wish to use Xavier trademarks, including logos, should consult the Xavier University Brand Platform and Style Guide to ensure compliance.

8. Using University computers for personal use

Students: While it is acceptable for students to use the University network resources for personal or recreational purposes such as social networking, playing computer games, chatting, or using personal email, academic work and University business always take priority. In a public computing environment, if nearby terminals are busy, staff or other Users may require a recreational User to relinquish the terminal for academic use, and recreational Users are expected to comply courteously.

Faculty and staff: Xavier recognizes that faculty and staff may use the University computer network for non-work or non-University-related purposes, such as attending to personal business, paying bills, or reading a website. Such incidental personal uses are permitted as long as they are not excessive, do not interfere with an employee's work, customer service, responsibilities of the workplace, or the necessary business of the University. Using Xavier equipment for inappropriate or excessive personal communications, or viewing web content that is inappropriate or illegal is prohibited. The University cannot guarantee that non-work-related items on Xavier systems will be maintained, nor do employees have a right of privacy in personal communications and files transmitted or stored on University information technology resources.

For Xavier staff, in general, personal uses are to be kept to a minimum and should be limited to breaks or lunch periods. There may be exceptions to this depending on work schedules and individual or department needs. Some individual departments may have their own policies regarding personal use of computing equipment. If there is any uncertainty, employees should consult their supervisor.

All Users should refrain from using Xavier's computing resources for financial gain, personal profit, or commercial purposes, unless prior authorization is granted. Exceptions are made for scholarly research that may produce revenue.

CONNECTING ONE'S OWN EQUIPMENT TO XAVIER'S NETWORK

Ability to access computing resources does not imply authorization to do so. Users who connect personal equipment (such as personal computers, smart phones, etc.) to the University network are responsible for the security of resources—not only against risks to the resources themselves but also against the possibility that unsecured resources can be misused by anyone on the Internet as a way to attack Xavier's systems.

Any misuse of one's own equipment through a user's neglect to provide safeguards may be reason to deny access for the equipment to Xavier's network. Users are encouraged to:

- Use strong passwords (consult the Information Resources Center for information on password requirements and the Xavier Password Manager);
- Limit access to the equipment;
- Keep files from unknown sources off of the equipment;
- Back up files;
- Use up-to-date antivirus software;
- Use great caution in opening email attachments from unknown senders;
- Keep operating system up-to-date;
- Keep application software updated;
- Turn off or delete unnecessary software features.

DISCLAIMER

Xavier is not responsible for the content of web pages other than the official web pages of University departments, divisions, and other units. The Website may include unmoderated public forums containing the personal opinions and other expressions of the persons who posted the entries. Neither the content of these forums nor any posted links to third-party websites are necessarily screened, approved, reviewed or endorsed by Xavier or any entity affiliated with Xavier. Xavier does not publish the content of the public forums or any content that may be available through links to and from them. Xavier is acting solely as an interactive computer service provider as defined under 47 U.S.C. § 230(f).

The text and other material on the Website reflect the opinion of the specific author and are not statements of advice, opinion, or information of Xavier.

Users may not use Xavier web pages for fundraising or advertising for commercial or non-commercial organizations, except for University-related organizations and University-related events, in compliance with policies governing these activities.

ENFORCEMENT

Violations of University policies governing the use of University electronic resources, including email services, may result in restriction of access to University information technology resources in addition to any disciplinary action that may be applicable under other University policies. These disciplinary measures may involve actions up to and including termination or expulsion, or civil or criminal liability. All users are encouraged to report any suspected violations of University computer policies to the Chief Information Officer. Users suspected of wrongdoing may have their information technology privileges restricted or suspended.

NOTIFICATION OF POLICY CHANGES

Xavier reserves the right to change the Policy on Acceptable Use of University Computers and Network Systems at any time. Such changes will be posted on the Xavier website (www.xavier.edu) and will become effective upon posting.

CONTACTING XAVIER

Please contact the IR Policy and Security Committee at irpsc@xavier.edu with any questions about this policy.

AUTHORITATIVE SOURCE

The authoritative source for this policy, and responsibility for its implementation, rests with the Chief Information Officer.

APPROVAL AND REVIEW HISTORY

Adopted by the Division of Information Resources' Policy and Security Committee: 1-7-2009
Reviewed and approved by the Information Resources Leadership Team: 1-20-2009
Reviewed and approved by the CIO: 2-13-2009
Reviewed by the University Technology Committee: 2-23-3009
Reviewed by the Academic Technology Committee: 2-27-2009
Placed on the MyXU portal for review and comment by the Xavier community: March 2009
Reviewed and approved by attorneys[1]: 6-22-2009
Reviewed and approved by the President's Cabinet: 3-2-2010

REVIEW CYCLE

This policy will be periodically reviewed and updated as appropriate.

[1] *Attorneys Jennifer Anstaett and John Li of Beckman-Weil-Shepardson, LLC reviewed and edited these policies during the month of June 2009*