**Xavier University Policies & Procedures Manual**

***Section 3: Employee Responsibilities***

**Policy: 3.06 ACCEPTABLE USE OF COMPUTERS AND NETWORK EQUIPMENT**

**Scope: Faculty and Staff**
**Responsible University Office: Information Technologies**
**Responsible Executive**
**Effective:** September 2013
**Last Update:**

**AUTHORITATIVE SOURCE**

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

**APPROVAL AND REVIEW HISTORY**

Drafted and reviewed: February 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
Revised by Information Technologies Policies and Procedures Task Force and Information Technologies Leadership Team: 2-2013

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

## A. PHILOSOPHY

This policy (hereafter the "Terms") establishes rules and strategies for acceptable use of Xavier University's (the "University") information technologies and resources, including, without limitation, the following:

1. All University-owned, operated, leased or contracted computing, networking, telephone and information resources, whether they are individually controlled, shared, standalone, or networked;
2. Physical facilities, including all hardware, software, applications, databases, and storage media;
3. All information maintained in any form and in any medium within the University's computer resources;
4. All University voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services; and
5. All creation, processing, communication, distribution, storage, and disposal of information by any combination of University resources and non-University resources (Hereinafter referred to collectively as "technology resources" or the "University's technology resources").

The policy is based on the following underlying principles:

- Technology resources are provided to support the essential mission of the University, including its teaching, scholarship, and service missions; administrative functions; student activities; and more.
- University policies, state and federal law, and other regulations govern the use of information resources.
- The information technologies infrastructure is provided for the entire University 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 technology resources 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 University employee, student, and affiliate who deals with technology resources. It is the responsibility of every User to read and understand the Terms and to conduct their activities accordingly. The Terms are in place to protect the University community. Inappropriate use exposes the University to risks including virus attacks, compromise of technology resources, and legal issues.

Individual departments and/or administrative units may have additional, supplemental policies regarding technology resources. Individual policies do not supersede, replace, or invalidate this policy.

**STATEMENT ON ACADEMIC FREEDOM**

Technology resources at the University 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 the University 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 technology resources , including but not limited to: all faculty, staff, students, alumni, retirees, temporary workers, library patrons, visitors, contractors, and vendors using University technology resources, whether on- or off-site (hereafter collectively referred to as "Users").

## B. POLICY

**UNIVERSITY RIGHTS**

The University reserves the right to access, monitor and disclose the contents and activity of an individual User on any technology resources and any Personal technology resources on University property connected to technology resources. This action may be taken for any reason, including, without limitation, the following:

1. Maintaining the network's integrity and the rights of others authorized to access technology resources,
2. Maintaining the security of technology resources if such technology resources are threatened;
3. Preventing misuse of technology resources if such misuse is suspected, or
4. Furthering a legitimate business need of the University (e.g., access to technology resources is necessary due to sudden death or incapacity of the employee).

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

**USER RIGHTS & RESPONSIBILITIES**

Members of the University community are granted access to 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:

- Course development and course management;
- Research projects and thesis preparation;
- Work of administrative departments;
- Communication with students, faculty, and staff at the University or at other academic institutions; and
- Communication within and outside the University for purposes related to the business of the University.

Users must c**omply 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.

**C. PROCEDURE**

The following examples, though not covering every situation, specify some of the rights and responsibilities that accompany use of technology resources at the University:

***1. Using limited resources responsibly and efficiently***

Users may not knowingly or intentionally engage in activities that could negatively impact the functionality of the University's technology resources. Users may only use the University's technology resources in the manner and to the extent authorized. Users are expected to promote efficient use of technology resources, consistent with the University's instructional, research, public service, and administrative goals. The University 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;
- 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 file sharing 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 University network through any computer or network device (including wireless access points);
- Establishing or maintaining a server without prior written authorization;
- Abusing printing privileges; or
- 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 Technologies Division's Project Management Office to ensure efficiency and compatibility with existing systems.

***2. Privacy and confidentiality***

The University provides technology resources to Users to effectively perform their job duties. The University will not routinely monitor an individual User's electronic data, software, or communication files.

Users are prohibited from using technology resources to infringe on others' privacy. Unauthorized reading, copying, or modification of files or email is prohibited. Users may not reveal confidential information obtained from technology resources 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 email, voicemail, and internet communications via chat or social networks such as Twitter and Facebook ("Electronic Communications") for University-related activities. However, those who use Electronic Communications 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.

The University 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 Help Desk at 745-HELP (4357).

***4. Information security***

Users are responsible and accountable for the security of the technology resources or Personal technology resources they own or use.

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 technology resources, and may not attempt to subvert the restrictions associated

with technology resources. Without regard to whether information on any technology resources (such as email, voicemail, or document files) is access-restricted, Users may not access any E-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 technology resources 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:

- Logging off or locking workstation when leaving one's desk,
- Backing up data regularly.
- Destroying drives, CDs, and other electronic media when they are no longer usable,
- Locking flash drives, CDs, and other electronic media in a desk or in a fire-resistant cabinet, and
- Taking special care to secure small portable devices (such as laptops and smart phones), which can be easily lost or stolen.

***6. Installation of software***

Users are responsible for using technology resources in accordance with copyright and licensing restrictions and applicable University policies. Users may not use University technology resources to violate copyright or the terms of any license agreement.

Most software available for use at the University 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 University 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 Terms outlined herein.

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 the University'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 the University's copyright policies.

The logo, name and graphics of the University or the University's affiliates are trademarks of the University or its affiliates. Use, reproduction, copying or redistribution of the University's trademarks, without the written permission of the University 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 the University's trademarks, including logos, should consult the Xavier University Brand Platform and Style Guide to ensure compliance.

***8. Using University technology resources for personal or non-organizational use***

Users may not use technology resources for any of the following reasons:

1. Outside work that is compensated by an entity other than the University, except as authorized by a University dean or the director of an administrative unit, or pursuant to an approved grant or sponsorship agreement;
2. The benefit of organizations not related to the University, except those authorized by a University dean or the director of an administrative unit, for appropriate University-related service;
3. Personal gain or benefit;
4. Political or lobbying activities not approved by the University; or
5. Private business or commercial enterprise.

University technology resources may not be used for commercial purposes, except as specifically permitted under other written policies of the University or with the written approval of a divisional vice president. Any such commercial use must be properly related to University activities and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use.

***Students:*** While it is acceptable for students to use the University technology 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 University technology resources 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, and do not interfere with an employee's work, customer service, responsibilities of the workplace, or the necessary business of the University. Using University technology resources 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 University technology resources will be maintained, nor do employees have a right of privacy in personal communications and files transmitted or stored on University technology resources.

For University 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 technology resources. If there is any uncertainty, employees should consult their supervisor.

***BRING YOUR OWN Personal technology resources***

Users who connect personal equipment such as tablets and iPads, Blackberries, iPhones, Android devices, other smart phones, laptops, etc.("Personal technology resources") to the University technology resources are responsible for the security of their Personal technology resources—not only against risks to the Personal technology resources themselves but also against the possibility that unsecured Personal technology resources can be misused by anyone on the Internet as a way to attack the University's technology resources. Any misuse of one's Personal technology resources through a User's neglect to provide safeguards may be reason to deny access for the equipment to University's technology resources, or additional sanctions as appropriate.

Users connecting Personal technology resources to access the University's Technology resources must abide by the following requirements:

- User will not download or transfer Sensitive University Data to their Personal technology resources. Sensitive University Data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual or the University, including information protected by the Family Educational Rights and Privacy Act of 1974 ("FERPA") and other regulations.

- User will password-protect and/or passcode-lock their Personal technology resources; Users must comply with all University password policies, including use of strong passwords, password expiration, and password history.
- User agrees to maintain the original operating system for their Personal technology resources and keep their Personal technology resources current with security patches and updates, as released by the manufacturer.
- User agrees that Personal technology resources will not be shared with other individuals or family members, due to the business use of the device.
- User will not download/transfer data that is considered sensitive or confidential to Personal technology resources.
- User agrees to delete any sensitive files that may be inadvertently downloaded and stored on Personal technology resources through the process of viewing e-mail attachments.
- If the Personal E-Resource is lost or stolen, the User will notify the Help Desk via phone or email within one hour, or as soon as practical after the User notices that the Personal E-Resource is missing. The Help Desk will wipe the memory of the E-Resource (Users are strongly encouraged to regularly back up their personal technology resources, so minimize loss in case a missing personal E-Resource must be wiped).
- User will maintain anti-virus protection on the Personal E-Resource.
- Users may only use approved and configured Virtual Private Network (VPN) client software.

**DISCLAIMER**

The University 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 the University or any entity affiliated with the University. The University does not publish the content of the public forums or any content that may be available through links to and from them. The University 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 the University.

Users may not use University 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 technology resources may result in one or more of the following actions:

1. User will be notified that the misuse must cease and desist.
2. The project or work will be more carefully supervised.
3. The User will be required to reimburse the University or pay for E-Resource(s).
4. The User will be denied access to the E-Resource(s), temporarily or permanently.
5. The appropriate University disciplinary action will be initiated. Actions may include sanctions, up to and including, termination of employment or expulsion.
6. Civil action will be initiated.
7. Law enforcement authorities will be contacted to initiate criminal prosecution.

**RELATED POLICIES**

Student Handbook
Faculty Handbook
Staff Handbook
HR Policies and Procedures Manual
Harassment Code and Accountability Procedures
Policy on the Privacy of Electronic Information
McDonald Library Responsible Use Policy
Gallagher Student Center Policy Manual
Policy on User Accounts

**NOTIFICATION OF POLICY CHANGES**

The University 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 University website (www.xavier.edu) and will become effective upon posting.

**REVIEW CYCLE**

This policy will be periodically reviewed and updated as appropriate. Policies should be reviewed at least every two years.