XAVIER UNIVERSITY

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

Effective: March 2022

Last Updated: September 2013

Responsible University Office: Information Technologies

Responsible Executive: Associate Provost and Chief Information Officer

Scope: Students, full time and adjunct faculty, staff, retirees, non-employee associates and guests

---

A. REASON FOR POLICY

A trusted and effective information technology environment ("IT environment") is vital to the mission of Xavier University ("University"). To that end, the University provides an IT environment which includes an array of institutional, computer hardware, electronic systems, computing services, networks, databases, and other resources (collectively, "IT Resources" or "Resources"). These Resources are intended to support the educational and work activities of members of the University's academic community and their external collaborators, support the operations of the University, provide access to services of the University and other publicly available information, and ensure a safe and secure IT operating environment to all members of the University community.

This policy is intended to define and promote the responsible use of information technology at the University while simultaneously limiting and preventing abuse of IT resources. Access to and usage of IT Resources entails certain expectations and responsibilities for both users and managers of the IT environment. This policy applies to all users of university technology resources ("Users"), regardless of affiliation and irrespective of whether these resources are accessed from Xavier's campus or from remote locations. Users covered by the policy include (but are not limited to) students, full time and adjunct faculty, staff, retirees, non-employee associates and guests of the University.

Access to IT 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 student, faculty, staff, retiree, non-employee associate, and guest of the University who interacts with IT resources. It is the responsibility of every User to read and understand the terms of this Policy and to conduct their activities accordingly.

The purpose of this Policy is to protect the University community. Inappropriate use of IT resources exposes the University to risks including cyber security attacks, compromise of IT resources, and legal issues.

B. POLICY

1. Appropriate Uses

Xavier University provides IT Resources to its community to facilitate University-related purposes, including, but not limited to, academic activities, service activities, student development, research, work, and campus life activities.

Examples of acceptable uses are:

- Course development and course management
- Research projects and thesis preparation
- Work of administrative departments
- Communication within and outside the University for purposes related to the business of the University

University owned data stored on electronic and computing devices, whether owned or leased by the University, an individual or a third party, remains the sole property of Xavier University.

2. Individual Responsibilities

Incidental Personal Use

The University allows incidental personal use of IT Resources. Such use must not consume significant IT resources, interfere with other users' access to resources, be excessive as determined by management, or otherwise violate any federal or state laws, or any University policies or codes of conduct.

Incidental personal use that inaccurately creates the appearance that the University is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

Users who make incidental personal use of IT resources do so at their own risk. The University cannot guarantee the security or continued operation of any IT resource or the security of any personal data.

If personal use adversely affects or conflicts with University operations or activities, the individual will be asked to cease those activities and may be subject to disciplinary actions.

Individual Responsibilities

When an individual accesses University computing services and accepts any University issued computing account, they agree to comply with this Policy and all other related policies. All members of the University community are responsible for familiarizing themselves with all applicable policies prior to use.

The University requires Users to engage in "safe computing" practices, such as establishing appropriate access restrictions for their accounts, setting strong passwords and guarding those passwords, keeping their personal operating systems and software applications up-

to-date and patched and employing security measures on their personal devices. Additional measures are described in other policies approved and posted on the Information Technology Policy website, including:

- Banner System Access Policy
- Cyber Security Incident Response Policy
- Electronic and Information Technology Accessibility Policy
- Information Classification Policy
- Information Security Policy
- Information Technology Acquisition and Disposal Policy
- Password Policy
- Policy on the Privacy of Electronic Information
- User Accounts Policy
- Web Privacy Policy

Users are responsible to prevent others from obtaining physical access to their IT resources and ensuring that electronic and paper files in their care are safeguarded.

Bring Your Own Device (BYOD)

Users connecting personal devices to IT resources must abide by the following requirements:

- Users will not download or transfer Sensitive University Data to their personal devices or unapproved cloud storage.
- Users will password-protect and/or passcode-lock their personal devices; Users must comply with all University password policies.
- Users agree to maintain the original operating system for their Personal devices and keep their personal devices current with security patches and updates, as released by the manufacturer.
- User agrees to delete any Sensitive University Data that may be inadvertently downloaded and stored on personal devices.
- If the personal device is lost or stolen, the device should be erased if possible. Contact the help desk to report the incident and to get assistance. Users are strongly encouraged to regularly back up their personal devices.
- Users will maintain appropriate security protection on the personal device.
- Users may only use approved and configured Virtual Private Network (VPN) client software when a VPN is required to access Xavier IT Resources (https://vpn.xavier.edu).
- Personal devices must not disrupt University services or bypass University established controls and safeguards.

Legal and University Compliance

When using IT resources or third-party owned resources, Users must comply with all applicable federal, state and local laws. These include laws of general application, such as libel, copyright, trademark, privacy, obscenity, and export control, for instance, the

Technology, Education, and Copyright Harmonization Act (TEACH Act) and the Digital Millennium Copyright Act (DMCA) as well as laws that are specific to computers and communication systems, such as the Computer Fraud and Abuse Act (CFAA) the Federal anti-hacking statute that prohibits unauthorized access to computers and the Electronic Communications Privacy Act (ECPA).

Intellectual honesty is of vital importance in the academic community. Users must not utilize IT resources to violate copyright, patent, trademark, other intellectual property rights, engage in plagiarism, or illegally download or share files. Upon formal notification or due to detection, IT must take down or otherwise block access to the infringing material.

Users must also comply with applicable University policies, and the terms of any contract or license which governs the use of the third-party resource and by which the Individual or the University is bound.

Unauthorized Use

Users will not engage in unauthorized use of IT resources. Users will use only computers, computer accounts and data for which they have authorization. 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.
- Allowing unauthorized access to the University network through any computer or network device (including wireless access points).

Use of equipment or devices that may negatively impact security, stability or performance of the University computing environment is prohibited.

Unauthorized use of a Xavier University user personal identity or access (log-in) credentials is prohibited, as is sharing of credentials between two or more users.

IT resources will not be used to fundraise, advertise, lobby, or solicit unless that use is Authorized by the University.

The use of IT Resources, like all other University-provided resources and activities, is subject to the requirements of ethical and legal behavior, which are consistent with University policy and federal, state and local law.

Users are prohibited from infringing others' privacy.

User are prohibited from sending obscene, pornographic, rude, or harassing messages of any kind.

The public display of sexually explicit material on any resource may constitute sexual harassment under Title IX and Xavier University’s sex discrimination policies.

Xavier University faculty, staff and students are protected from sexual harassment by federal law; compliance is administered by Xavier University’s Title IX Office.

Users may not use IT Resources to access or possess pornographic material unrelated to university instruction, research, or business needs.

Users are prohibited from using IT resources in any way that would suggest institutional endorsement.

IT resources shall not be used to operate a business or for commercial purposes unless that use is approved in advance by the appropriate University senior leader.

IT resources may not be used to support the operations or activities of organizations that are not affiliated with the University unless authorized by Xavier University.

Users are prohibited from establishing or maintaining a server without prior written authorization from Information Technologies. If approved, users are required to be responsible for keeping the server up-to-date and free of vulnerabilities.

Users are prohibited from launching attacks, probes, or introducing, creating, or propagating any malicious programs.

Users are prohibited from abusing printing privileges.

Use of Enterprise Tools

The University purchases and maintains enterprise collaboration, social media, learning, research, and other technology platforms. Faculty and staff should leverage these enterprise tools available to them in the University technology ecosystem. The use of enterprise tools reduces the risk to the University and increases compliance with university policies, procedures, standards and guidelines, and applicable regulatory requirements.

3. University Rights and Responsibilities

The University reserves the right to access, monitor, and disclose the contents and activity of an individual User on any University IT resources and any personal device connected to or interfering with University IT resources. Such actions may be taken at the institutional or local level and may include, but are not limited to, scanning, sanitizing, or monitoring stored data, network traffic, usage patterns and other uses of IT Resources. It may also include blocking unauthorized access to and unauthorized uses of its networks, systems, and data.

This action may be taken for any reasonable cause, including, without limitation, the following:

- Maintaining the network's integrity and the rights of others authorized to access IT Resources.
- Maintaining the security of IT Resources from threat or suspected threat;
- Preventing misuse of technology if such misuse is suspected; and
- Furthering a legitimate business need of the University (e.g., access to IT Resources is necessary due to sudden death or incapacity of the employee).

Additionally, the Office of Information Technologies may investigate based on the request of Office of General Counsel, XUPD, Human Resources, Office of Student Affairs, Office of the Provost and Chief Academic Officer or Office of the President. If a violation of any applicable laws, regulations or policies is discovered during such an investigation, the Office of Information Technologies will contact other appropriate university departments for further action.

Users who violate the Policy may be subject to disciplinary action handled through the University's normal student and employee disciplinary procedures.

C. DEFINITIONS

Users: All individuals that have access to Xavier's IT Resources, including but not limited to all students, full time and adjunct faculty, staff, retirees, non-employee associates and guests using Xavier University IT Resources, whether on or off site.

IT Resources: Includes an array of institutional electronic systems, computing services, networks, databases, and other resources (collectively, "IT Resources" or "Resources").

Sensitive University Data: 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"), General Data Privacy Regulation (GDPR), other privacy regulations and data classification policies.

Family Education Rights and Privacy Act (FERPA): FERPA of 1974 as amended details the access of student records held and maintained by educational institutions. More information can be found on the *Xavier University Registrar's FERPA web site*.

General Data Protection Regulation (GDPR): GDPR governs the way in which we can use, process, and store personal data (information about an identifiable, living person). It applies to all organizations within the European Union (EU), as well as those supplying goods or services to the EU or monitoring EU citizens.

Technology, Education, and Copyright Harmonization Act (TEACH Act): modifies section 110(2) of the Copyright Act and allows for transmission of copyrighted works in distance education, online classes, and digital course management systems provided certain conditions are met.

Digital Millennium Copyright Act (DMCA): sets forth a general prohibition on circumvention of technological measures that control access to a digital work even if the resulting use of the work would otherwise be fair use.

Misuse: Technology or Data not used as intended based on policy, legal compliance or as defined in the Unauthorized Use or BYOD section.

D. PROCEDURES

Reporting and Enforcement

An individual's access to IT Resources may be limited, suspended, or terminated without warning if that individual violates this or any other University policy. Alleged or suspected violations of this policy will be addressed by the Office of Information Technologies and referred to the appropriate Xavier University department. Violations of University policies governing the acceptable use of IT Resources may result in action against the User.

The Office of Information Technologies reserves the right to remove or disconnect any device from IT Resources if such device negatively impacts, or has the potential to negatively impact, university operations as determined by the Office of Information Technologies.

Investigations of information technology systems or services misuse is limited only to the Office of Information Technologies or their designee. In addition to its own administrative review of possible violations of this policy and other university policies, the University is obligated to report certain uses of IT resources to law enforcement agencies. If an investigation involving review of the content of a faculty member, staff member or student's files is required, authorization will be obtained from the Office of General Counsel or other appropriate departments, as necessary. Disciplinary action for violation of this policy is handled through the University's normal student and employee disciplinary procedures.

Technical Issues

For technical issues send a request to the Information Technologies Help Desk at helpdesk@xavier.edu or 513-745-4357.

Grievances

Grievances for decisions made regarding this policy should be sent to the Associate Provost and Chief Information Officer.

E. EXHIBITS (N/A)

F. 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: 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
Updated and reviewed: 9-12-2019
Updated and reviewed: 10-12-2020
Updated and reviewed: 1-4-2022

DISCLAIMER

The University is not responsible for the content on websites or social media pages, other than the official web pages (https://xavier.edu), of university departments, divisions, and other units ("unofficial websites"). Such unofficial websites may include unmoderated public forums containing the personal opinions and expressions which do not represent the opinions or expressions of Xavier. The content of these unofficial websites and any links posted to third-party websites are not screened, approved, reviewed, or endorsed by the University or any entity affiliated with the University. The text and other material on the unofficial websites reflect the opinion of the specific author and are not statements of advice, opinion, or information of the University.

No one may 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.

RELATED POLICIES, HANDBOOKS AND GUIDELINES

- Student Handbook
- Faculty Handbook
- Staff Handbook
- HR Policies and Procedures Manual
- Harassment Code and Accountability Procedures
- University Library Acceptable Use Policy
- Copyright Resources for Faculty
- Copyright Resources for Students
- Gallagher Student Center Policy Manual
- Banner System Access Policy
- Cyber Security Incident Response Policy
- Electronic and Information Technology Accessibility Policy
- Information Classification Policy
- Information Security Policy
- Information Technology Acquisition and Disposal Policy
- Password Policy
- Policy on the Privacy of Electronic Information
- User Accounts Policy
- Web Privacy Policy

NOTIFICATION OF POLICY CHANGES

The University reserves the right to change the Policy on Acceptable Use of IT Resources 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.