Xavier University Policies & Procedures Manual

Section 3: Employee Responsibilities

Policy: 3.xx POLICY ON THE PRIVACY OF ELECTRONIC INFORMATION

Effective: February 2013
Last Update:

Responsible University Office: Information Technologies
Responsible Executive
Last Reviewed Date: June 2014

Scope: Faculty, Staff and Students

CONTACT

Please contact the Executive Director of Infrastructure and Technology Support 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

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
Technologies Leadership Team: 6-2014

[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 is Xavier University's (the "University") policy relating to the privacy and confidentiality of electronic information and email. This policy seeks to balance individual freedom and privacy with the operational needs of the University.

Users are reminded that all uses of the University's information technology resources, including email, are subject to all relevant University policies and state and federal laws, including copyright law.

B. POLICY

The University discourages the storage of sensitive or confidential information on portable storage devices (either personal or University-owned). However, if any sensitive data is maintained on a portable storage device, users are required to password-protect and/or passcode-lock the device, and or encrypt/restrict such documents and emails with industry standard encryption. FERPA and HIPAA covered information should not be stored to portable devices. For more information about responsibilities for protecting sensitive or confidential information on portable devices, see the Acceptable Use Policy for University Computers and Network Systems or contact the Help Desk at 745-HELP (4357).

If sending confidential or highly sensitive information via email, it is recommended that these documents be encrypted and/or configured for restricted access. For information on restricting documents through password-protection or encryption, please contact the Help Desk at 745-HELP (4357).

Please note that email in its present form is never completely secure and is potentially vulnerable to unauthorized access by third parties. Receivers of email should check with the sender if there is any doubt about the sender's identity or the email's authenticity.

Users of email should keep in mind that even if the sender and recipient have discarded their copies of an email record, there may be back-up copies of such email that can be retrieved on University systems or any other electronic systems through which the data has traveled.

University email services may be used for incidental personal purposes provided such use does not violate the University's Policy on Acceptable Use of University Computers and Network Systems.

As long as a user's account is active, there is no restriction against printing, copying or manually forwarding memos or files, provided that such copying/forwarding does not compromise confidentiality, or violate any University policy or any local, state or federal laws.

C. DEFINITION OF ELECTRONIC INFORMATION

This policy covers:

- Any information that is created or transmitted electronically, including all electronic data, documents and files, electronic mail, telecommunications & voice mails, faxes, databases, web pages, information submitted online, and information stored on individual computers or voice mail accounts, on University-owned systems/devices.
- University administrative data and other University files on personally owned devices.

D. PROCEDURES

The University takes reasonable precautions to preserve user privacy and to secure its systems, but the University cannot guarantee the security of electronic data stored, sent, or received on University-owned equipment.

Although the University limits access to shared folders to authorized individuals, discretion should be used when storing sensitive or confidential information in group (shared) folders.

AUTHORIZED ACCESS TO ELECTRONIC INFORMATION

On rare occasions, it may be necessary for authorized personnel to access electronic mail, files, and data stored on the University's computers or networks to ensure the orderly administration and functioning of our information resources. The University does not routinely monitor electronic mail, files, or data. The University does use automated tools and utilities that either scan network traffic, or scan the information on University managed servers. The University reserves the right to access user electronic mail, files, or data on the University's servers when the University determines such access is necessary and appropriate. These occasions are an exception basis and are not routine. Examples of necessary and appropriate access include, without limitation, the following purposes:

1. Troubleshooting hardware and software problems;
2. Preventing or investigating unauthorized access and system misuse;
3. Retrieving electronic mail, files, or data in emergency circumstances where there is a threat to health, safety, or University property, or if there is substantial risk of harm or liability;
4. Retrieving a former employee's electronic mail, files, or data by the unit to which the employee was assigned, as necessary (e.g., to respond to students, customers and vendors who may continue to send emails to that address);
5. Retrieving electronic mail, files, or data of a deceased or incapacitated employee;
6. Providing access to electronic mail, files, or data to a lawful representative (e.g., spouse, parent, executor, holder of power of attorney) of a deceased or incapacitated employee or student;
7. Investigating reports of violation of University policy, or local, state, or federal law;
8. Investigating reports of misconduct; and
9. Complying with requests for information when litigation is threatened or pending.

When accessing user electronic mail, files, or data, the University will make reasonable efforts to notify the affected user, except when such notification may be inappropriate, impractical, or unlawful.

Units and departments are encouraged to make arrangements for disposition of electronic mail, files, and data with departing employees and students in advance of their departure.

For more information about the retention of accounts and electronic mail, files, or data when an employee leaves employment or a student graduates or otherwise withdraws from the University, see the separate Policy on User Accounts.

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.

RELATED POLICIES

Acceptable Use Policy for University Computers and Network Systems
Student Handbook
Faculty Handbook
Staff Handbook
HR Policies and Procedures Manual
Policy on User Accounts

NOTIFICATION OF POLICY CHANGES

Xavier reserves the right to change the Policy on the Privacy of Electronic Information at any time. Such changes will be posted on the Xavier 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.