POLICY: ACCEPTABLE USE

DOCUMENT#: POL-0001
EFFECTIVE: February 2023
REVIEWED: March 2025
OWNER: ISO

PURPOSE

Illinois Wesleyan University (IWU)'s technology infrastructure exists to support the institution and administrative activities needed to fulfill the institution's mission. Access to these resources is a privilege that should be exercised responsibly, ethically and lawfully.

The purpose of this Acceptable Use Policy is to clearly establish each member of the institution's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives will enable IWU to implement a comprehensive system-wide Information Security Program.

SCOPE

This policy applies to all users of computing resources owned, managed or otherwise provided by the institution. Individuals covered by this policy include, but are not limited to all faculty, staff, students, student workers, service providers, and guests with access to the institution's computing resources and/or facilities. Computing resources include all IWU owned, licensed or managed hardware and software, email domains and related services and any use of the institution's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

PRIVACY

IWU will make every reasonable effort to respect a user's privacy. However, faculty, staff, students, student workers, service providers, and guests do not acquire a right of privacy for communications transmitted or stored on the institution's resources. Additionally, in response to a judicial order or any other action required by law or permitted by official IWU policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the University President may authorize an IWU official or an authorized agent to access, review, monitor and/or disclose any available data associated with an individual's account, including stored files, network traffic, and internal logs. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or the institution's rules, regulations or policies, or when access is considered necessary to conduct IWU business due to the unexpected absence of faculty, staff or student workers or to respond to health or safety emergencies.

POLICY

Activities related to the IWU mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the institution's mission is prohibited.

Following the same standards of common sense, courtesy and civility that govern the use of other shared facilities, acceptable use of information technology resources generally respects all individuals' privacy, while protecting the right of individuals to be free from intimidation and/or harassment. All users of IWU's computing resources must adhere to the requirements below.

These requirements are in addition to any requirements regarding behavior or conduct defined in other University policies and procedures such as the Faculty and Staff handbooks or Student Code of Conduct, and it does not supersede them.

Unacceptable Use

All users are prohibited from using Illinois Wesleyan resources in a manner which results in a violation of law or University policy or potentially adversely affects network service performance. Examples of Unacceptable Use include the following:

- Activity that violates federal, state, or local law
- Activity which violate any University policy or procedure
- Activities that lead to the destruction or damage of data, equipment, or reputation of others or the University
- Circumventing University information security controls
- Intentionally installing malicious software
- Impeding or disrupting the legitimate computing activities of others
- Unauthorized use of accounts, access codes, passwords, or identification numbers
- Unauthorized use of systems and networks
- Unauthorized monitoring of communications
- Unauthorized use of IT Resources for commercial purposes
- Transmitting commercial or personal advertisements, solicitations, or promotions

INCIDENT REPORTING

IWU is committed to responding to security incidents involving personnel, institution-owned information or institution-owned information assets. As part of this policy:

- The loss, theft or inappropriate use of institution access credentials (e.g. passwords, key cards or security tokens), assets (e.g. laptop, cell phones), or other information should be reported to the IT Service Desk.
- No faculty, staff, student worker, or vendor will prevent another member from reporting a security incident.

MESSAGING

The institution provides a robust communication platform for users to fulfill its mission. Users must not:

- Send unsolicited electronic messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (spam);
- Solicit electronic messages for any other digital identifier (e.g. e-mail address, social handle, etc.), other than that of the poster's account, with the intent to harass or to collect replies; or
- Create or forward chain letters or messages, including those that promote "pyramid" schemes of any type.

OTHER

In addition to the other parts of this policy, users must comply with any requests regarding usage of IWU IT resources as delivered by the University IT staff.

ROLES AND RESPONSIBILITIES

IWU reserves the right to protect, repair, and maintain the institution's computing equipment and network integrity. Any information obtained by IT personnel about a user through routine maintenance of the institution's computing equipment or network will remain confidential, unless the information pertains to activities that are not compliant with acceptable use of IWU's computing resources.

ENFORCEMENT

Enforcement is the responsibility of the University IT department or designee. Users who violate this policy may be denied access to the institution's resources and may be subject to penalties and disciplinary action both within and outside of IWU. The institution may temporarily suspend or block access to an account, prior to the initiation or completion of disciplinary procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect IWU from liability.

EXCEPTIONS

Exceptions to the policy may be granted by the Chief Information Officer, or by his or her designee. All exceptions must be reviewed annually. Any exception granted by the Chief Information Officer shall be communicated in writing to the respective Vice President within one (1) business day of the exception being granted.

9.0 RELATED POLICIES

- Information Security Policy
- Data Classification Policy
- Data Classification and Handling Procedure
- Faculty Handbook
- Staff Handbook
- Student Code of Conduct

10.0 RESPONSIBLE DEPARTMENT

Information Technology Security