Policy IT001: Acceptable Use Policy

Recommended for Approval by: Fawn Petrosky, Interim Vice President for Administration and Finance

Approved by: Dr. Dale-Elizabeth Pehrsson, President, Pennsylvania Western University;

Pennsylvania Western University Executive Cabinet

Effective Date: 07/01/2022

A. Intent

This policy applies to all users including faculty, staff, students, contractors and guest users of the Pennsylvania Western University (PennWest) computer network resources, equipment, or connecting resources. Use of the University's Information Technology Resources signifies agreement to comply with this policy.

While the University recognizes the role of privacy in an institution of higher learning and will attempt to honor that ideal, there should be no expectation of privacy of information stored on or sent through University-owned information technology, unless the law establishes a privacy right that is enforceable against the University. There may be instances where the University may be required to provide information stored in its Information Technology Resources to someone other than the user as a result of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.). Information stored by the University may also be viewed by technical staff working to resolve technical issues.

The purpose of this policy is to address the use of University issued/owned Information Technology Resources.

PennWest provides numerous Information Technology Resources for use by the University's students, faculty, and staff. The term Information Technology Resources includes, but is not limited to, all University computing equipment, storage devices, and any electronic device issued by the University and intended for business purposes, as well as software, systems, and networks. The use of Information Technology Resources includes the electronic communications over and through such devices. These resources are provided to support the University's mission and institutional goals. The use of these systems is a privilege and all users are expected to act responsibly and to follow the University's policies and any applicable local, state and federal laws (e.g., copyright, criminal use of a communication device, harassment, etc.) related to the use of these resources.

B. Definition(s)

User – a.k.a "end user". Any individual who uses a computer or other information technology resource that is controlled, managed or owned by Penn West.

C. Policy

- **Responsibilities of User of University Information Technology Resources:**
  - Respect the intellectual property rights of authors, contributors, and publishers in all media;
  - Protect user identification, password, information and system from unauthorized use;
  - Report lost or stolen devices, including devices that contain private or University information to IT immediately upon discovery of the loss;
  - Adhere to the terms of software licenses and other contracts. Persons loading software on any University computer must adhere to University contracting requirements and all licensing requirements for the software. Except where allowed by the University site licenses, copying software licensed for University use for personal use is a violation of this policy;
  - Adherence to all other applicable University policies and/or terms of any collective bargaining agreement;
  - To use the University Information Technology Resources in a manner that complies with State and Federal law. Adherence to all other applicable University policies and/or terms of any collective bargaining agreement;
  - Participate in required Security Awareness Training to learn how to better protect University Accounts, Systems, and Data.

- **Prohibited Uses of University Information Technology Resources:**
  - Providing false or misleading information to obtain a University computing account, or hiding or disguising one's identity to avoid responsibility for behavior in the use of information technologies;
  - Unauthorized use of another user's account, to include account sharing;
  - Attempting to gain or gaining unauthorized access to University Information Technology Resources, or to the files of another;
  - Performing any act(s) that impede the normal operation of or interfere with the proper functioning of University Information Technology Resources;
  - Interfering with the security mechanisms or integrity of the University's Information Technology Resources;
  - Use of the University Information Technology Resources to transmit material, chain letters, spam, or communications prohibited by state or federal law;
  - Transmitting or displaying media content in a manner that violates the University's sexual harassment policy;
  - Copyright infringement, including illegal file sharing of video, audio, software or data;

- Excessive use that overburdens the Information Technology Resources to the exclusion of other users;
- Personal use by employees that interferes with an employee's ability or availability to perform thier job responsibilities;
- Use of the University Information Technology Resources for personal profit, commercial reasons, non-University fundraising, political campaigns or any illegal purpose;
- The prohibition against using University Information Technology Resources for personal profit does not apply to:
    - Scholarly activities, including the writing of textbooks or preparation of other teaching material by faculty members; or
    - Other activities that relate to the faculty member's professional development.
    - Other activities as approved by the University President
- Non-authorized solicitations on behalf of individuals, groups, or organizations are prohibited;
- Intentionally or knowingly installing, executing, or providing to another, a program or file, on any of the University's Information Technology Resources that could result in the damage to any file, system, or network. This includes, but is not limited to computer viruses, malware, killware, ransomware, Cryptomining, Trojan horses, worms, spyware or other malicious program(s) or file(s).

- **Copying and copyright infringement:** the University respects and upholds the rights of holders of copyrights, their agents and representatives. It is the responsibility of employees and students to be aware of the rights of copyright owners. Legal use of copyrighted material can include, but is not limited to, ownership, license or permissions, and fair use under the US Copyright Act. Illegal use includes:
    - Reproducing or allowing others to reproduce copyrighted software material in any form without proper authorization, or not in keeping with the University's copyright regulations or federal and state laws.
    - The use of software applications that allow for the direct sharing of copyrighted works without the permissions of the copyright holder.
- **Email Communication:** The PennWest email system is considered an official means of communication and all students and employees are responsible for information sent to them via their PennsWest account. All students and employees are given a PennWest email account. With respect to those email accounts:
    - It is the responsibility of the email account owner to delete unwanted messages and attachments, and to otherwise maintain their account.
    - Students, Faculty, and Staff must use their University e-mail account for all University business. In order to protect University information and clearly distinguish official University business as opposed to personal communications, users are not permitted to use non-university email accounts (e.g. personal gmail, yahoo, Comcast, etc.) to conduct University business. Students, Faculty,

and Staff e-mail accounts may not be configured to redirect e-mail to personal accounts (gmail, yahoo, other e-mail providers) nor may students, faculty, and staff personal accounts be configured to send e-mail on behalf of their PennWest e-mail account.
    - It is expected that students and employees will check their PennWest email accounts on a frequent and consistent basis.

- **Enforcement:**

  A University employee or student who violates this policy risks a range of sanctions imposed by relevant University disciplinary processes, ranging from denial of access to any or all Information Technology Resources up to and including termination (for an employee) or dismissal (for a student). They also risk referral for prosecution under applicable local, state or federal laws.

  Enforcement of this policy may be subject to the terms and conditions of the various collective bargaining agreements that apply to faculty and staff.

D. Procedure(s)

Not applicable.

E. Related policies

Not applicable.

F. Contact Information

Information Technology Services

G. Policy Review Schedule

Contact office responsible for dates.