COMMONWEALTH UNIVERSITY OF PENNSYLVANIA

Acceptable Use of Technology

Policy Number 8-07

Commonwealth University of Pennsylvania

Approved by University Senate, November 13,

2025 Issued by Interim President Jeffery Osgood,

12/05/2025 Responsible Office: Office of

Technology

Previous Policy: PRP 2550

1. Purpose

1.1 This policy addresses the use of university issued/owned information technology resources.

1.2 Commonwealth University 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, cellular phones, storage devices, and any electronic device issued by the university and intended for business purposes, as well as software, local systems, cloud systems, and networks. 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 communication device, harassment, etc.) related to the use of these resources and the data they contain.

2. Scope

2.1 This policy applies to all users including faculty, staff, students, contractors and guest users of the Commonwealth University computer network resources, equipment, or connecting resources. Use of the university's information technology resources signifies agreement to comply with this policy.

2.2 While the university recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned information technology, except as required by state or federal law. For example, 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 and to audit for compliance.

2.3 This policy is subject to the terms and conditions of the various collective bargaining agreements that apply to faculty and staff.

3. Definitions, Roles and Responsibilities

3.1. **Definitions**

3.1.1. Authorized use: shall mean official permission for an event or action to happen, or the act of giving someone official permission to perform an event or action.

3.2. **Roles and Responsibilities**

3.2.1. The Office of Information Technology defines the Acceptable Use of Information Technology Resources in consultation with the Information Technology Senate Subcommittee.

4. Policy

4.1. Acceptable Use of Information Technology Resources

4.1.1. 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 as soon as the discovery of the loss occurs;

Adhere to the terms of software licenses and other contracts. Persons loading software on any University computer must adhere to all licensing requirements for the software and the software must be approved software that is inventoried on the University authorized software list. Except where allowed by the university site licenses, copying software licensed for university use for personal use is a violation of this policy;

Adhere to regulations and policies when working with AI-enabled software, in order to protect sensitive data from accidental exposure;

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.

4.1.2. 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 such as parents or guardians signing into a student's account as well as a student logging onto another student's account;

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 abusive, threatening, or harassing material, chain letters, spam, inappropriate disclosure of sensitive information, or other communications prohibited by state or federal law;

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;

Excessive or prohibited personal use by employees;

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:

i. Scholarly activities, including the writing of textbooks or preparation of other teaching material by faculty members; or

ii. Other activities that relate to the faculty member's professional development.

iii. 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, 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, Trojan horses, worms, spyware or other malicious program(s) or file(s).

5. Procedures, Standards, and Guidelines

6. Compliance and Enforcement

6.1. Every University policy will undergo a regular review on a five-year cycle, with approximately 20% of the total policies inventory being reviewed each year.

6.2. All policy reviews will be conducted by the responsible Senate Committee to assure that the policy remains relevant and aligns with applicable federal and state laws and regulations, PASSHE Board of Governors policies, and other University policies, procedures, standards, or guidelines.

6.3. 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). He or she also risks referral for prosecution under applicable local, state or federal laws.

7. Additional Information

7.1.1. Supporting Documents

7.2. History

7.2.1. This will replace PRP 2550 – Acceptable Use of Technology Policy issued by Dr. Richard Rugen, Vice President for Administration and Finance April 21, 2010.

7.2.2. Effective Date – [Date Approved by the University Senate or Issued by the Office of the President as an Interim Policy]

7.2.3. 10/8/2025

7.2.4. Next Review Date - [Date of Revision]

7.3. Related Policies

7.4. Contacts for Additional Information and Reporting

Office of Technology, Commonwealth University, Attn: Chief Information Officer, InformationTechnology@commonwealthu.edu