Millersville University **Governance & Policies**

**Effective: November 3, 2025**

**Information Technology Policy**
**RESPONSIBLE USE OF INFORMATION TECHNOLOGY RESOURCES**

**Approved: April 28, 2009**
**Updated November 3, 2025**
**President's Cabinet**

# 1. Introduction

Millersville University recognizes the importance of information technology (IT) in fulfilling its mission of teaching, learning, research, and public service. Information technology resources are essential for academic scholarship, administrative efficiency, and collaboration within and beyond the University. These resources support communication, instruction, research, and innovation, enabling the University to serve students, faculty, staff, and the wider community.

The University provides information technology resources for the primary purpose of conducting official University business, including academic, research, and administrative functions. Limited personal use is permitted, provided it does not interfere with institutional operations, violate laws or University policy, or incur costs to the University.

This policy applies to all students, faculty, staff, contractors, and guests who access Millersville University's IT systems, including but not limited to networks, computing devices, software, cloud-based services, and data storage.

# 2. General Use of IT Resources

Millersville University's information technology resources are provided to support the University's mission of teaching, learning, research, and public service. These resources are essential for academic and administrative operations and must be used responsibly, ethically, and in compliance with University policies and applicable laws. This section outlines the general expectations for access, accountability, security, and appropriate use of University IT systems.

## 2.1 Access and Accountability

IT resources are provided primarily for academic, research, and administrative purposes. Limited personal use is permitted, provided it does not interfere with institutional operations, violate University policy, or incur costs to the University. Users are responsible for safeguarding their credentials, may only use accounts assigned to them, and must not attempt to access systems, data, or accounts for which they are not authorized.

## 2.2 Privacy and Security

The University values academic freedom and privacy but reminds users that there is no expectation of absolute privacy when using University IT resources. The University will not routinely monitor individual accounts; however, it reserves the right to access or disclose information when required for legal compliance, security investigations, or operational necessity, in accordance with applicable laws such as Pennsylvania's Right-to-Know Law. Users must handle confidential, sensitive, or personally identifiable information (PII) in accordance with University data governance policies and applicable regulations (e.g., FERPA, HIPAA).

## 2.3 Email and Digital Communication

University-provided email and communication systems are intended for academic, research, and administrative purposes. Prohibited uses include:

- Sending chain letters, spam, or unauthorized mass mailings.
- Advertising or soliciting for personal business ventures or commercial enterprises.
- Transmitting unlawful, obscene, or harassing content.
- Distributing malicious or pirated software.

## 2.4 Network Use

All users must act responsibly to maintain the integrity of University networks. Prohibited activities include:

- Intentionally introducing malware, viruses, or other malicious code.
- Attempting to circumvent security controls or gain unauthorized access.
- Deliberately monopolizing network resources (e.g., excessive mass mailings, unnecessary printing, or resource-heavy processes that impair others' access).

### 2.5 Webpages and Online Publishing

Faculty, staff, and students may create personal or departmental webpages consistent with the University's mission and academic purposes. Such pages must comply with University policies and applicable laws, and may not misrepresent the University or disclose confidential information.

### 2.6 Software Licensing and Copyright

Users must comply with all software licensing agreements and copyright laws. Unauthorized copying, distribution, or installation of copyrighted or licensed software is prohibited. Site-licensed software may not be used for personal gain or distributed outside the University community.

## 3. Social Media Use and Online Communication

This section governs the responsible use of social media platforms and online communication channels when representing the University in an official capacity. All employees, including student employees, use should reflect professionalism, respect for others, and compliance with University policies.

### 3.1 University Representation

- Employees using social media for official University communications must follow brand guidelines from University Communications and Marketing (UCM).
- Initial registration of social media accounts should be done in consultation with University Communications and Marketing. Personal social media use shall not imply University endorsement of personal opinions or external entities.

### 3.2 Responsible Engagement

- Users must not engage in harassment, hate speech, or misinformation using University IT resources.

### 3.3 Privacy Considerations

- Employees should be aware that social media content, even on private accounts, may have reputational consequences and impact University relationships.
- Employees must not share confidential or sensitive University information on social media.

# 4. Compliance and Enforcement

The University is committed to ensuring that its information technology resources are used in a manner that upholds security, integrity, and compliance with institutional, state, and federal requirements. This section outlines the processes for addressing policy violations, reporting concerns, and maintaining ongoing review to adapt to evolving technology and regulations.

## 4.1 Violations and Reporting

- Sanctions for violations may include, but are not limited to, disciplinary processes as outlined in the Student Code of Conduct, Faculty Handbook, or Human Resources policies.
- Individuals subject to enforcement actions will be afforded due process consistent with University procedures, including the right to appeal decisions through established channels.
- The University may cooperate with external authorities when policy violations involve potential criminal activity, data breaches, or violations of federal/state law
- Suspected violations may be reported to the Chief Technology Officer, University Police, Human Resources, or other appropriate offices depending on the nature of the incident.
- Reports of policy violations and enforcement actions will be documented and retained in accordance with University records management policies.

## 4.2 Policy Review

This policy will be reviewed on a regular basis, at least every three years, to ensure alignment with evolving technology, legal requirements, and University needs.

# 5. Related Policies and References

- PASSHE IT Acceptable Use Policy
- Student Academic Dishonesty Policy
- Faculty Policy Academic Dishonesty and Plagiarism
- Electronic Data Classification and Handling
- University Institutional Review Board
- **Americans with Disabilities Act Title II Regulations**
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)