Acceptable Use Policy

PURPOSE

Information assets including data, computing devices, systems technology, telephony, and IT resources are vital to Shepherd University's ongoing mission of discovery, learning, and engagement. To support its mission, Shepherd University makes information assets and IT resources available (1) to facilitate operations, (2) to support scholarship, research, and instructional activities of faculty, (3) provide access to services, and (4) to support student and campus life activities.

POLICY

Shepherd University information assets including data, computing devices, systems technology, telephony, and IT resources shall be used in an approved, ethical, and lawful manner to avoid loss and/or damage to Shepherd University data, operations, image, or financial interests. All affiliated information/technological data should be considered as confidential and proprietary, thus every effort to protect its integrity should be made.

Brief, incidental and non-recurring personal use of IT resources is tolerated as part of daily learning and work of all members of the campus community, provided that such use does not violate any other applicable law, copyright infringement, or Shepherd University policy, procedure, and/or regulation.

As a condition to being granted use of or access to information assets and IT resources, each user (1) consents to the provisions of this policy and (2) agrees to comply with all of the terms and conditions detailed within this policy.

The following usage of IT resources are prohibited:

1. Circumvention of any security measure of Shepherd University or any measure that may violate any local, state, or federal law.

2. Intentional use, distribution or creation of viruses, worms, malicious software, ransomware, or other keylogging techniques.
3. Distributing denial of service (DoS) practices or any other device/system, program, or practice of a malicious motive.
4. Unauthorized use, copying, or distributing of licensed software or other copyrighted materials.
5. Intentional storage of Shepherd University data in an unsecure location.
6. Deliberately sending frivolous, excessive, or harmful electronic messages (e.g. phishing or spam).
7. Accessing information assets and/or other data that is not publicly available, does not belong to the user, and for which the user does not have explicit permission to access.
8. Accessing information assets or IT resources in a manner designed to circumvent access limitations on restricted or sensitive data (e.g. replicating databases) without permission.
9. Transmitting, receiving, accessing, printing, or storing any communication or other content of a defamatory, discriminatory, harassing, obscene, or sexually explicit nature.
10. Use of IT resources for any unauthorized commercial/personal business or organized political activity that is inconsistent with Shepherd University tax-exempt status or serves as a conflict of interest.

Use of information assets and IT resources is a privilege and not a right. All users are responsible for the actions performed on or transmitted with any Shepherd University information asset and/or IT resource. Violations of this policy, or any other Shepherd University policy, may result in revoked or limited technology privileges, as well as other disciplinary action up to and including expulsion, termination, or referral to appropriate authorities.

PRIVACY, OPERATIONS, and MONITORING

Shepherd University seeks to maintain its IT environment and manage all information assets including data, computing devices, systems technology, telephony, and IT resources in a manner that respects individual privacy and promotes user trust. However, the use of Shepherd University IT resources is not completely private, and users should have no expectation of privacy in connection with the use of any information asset or IT resource.

Shepherd University has the legal right to access, preserve, and review all information stored on or transmitted through any information asset or IT resource, including the inspection of e-mail messages, logging of activities, monitoring usage patterns, and data audits/integrity checks. IT Services may, with or without notice to users, take any other action it deems necessary to preserve, secure, and protect systems, information assets, or IT resources for the

betterment of Shepherd University. Without limiting its right to take action, Shepherd University may, at its sole discretion, disclose the results of any general or individual monitoring or access permitted by this policy, including the contents and records of individual communications, to appropriate Shepherd University personnel and/or law enforcement agencies.

SCOPE of AFFECTED PARTIES

This policy applies to all users, such as students, faculty, and staff of Shepherd University and to other persons accessing Shepherd University information assets and/or IT resources including but not limited to authorized agents or community members, regardless of whether such information asset or IT resource is accessed from on-campus or off-campus.

ROLES & RESPONSIBILITIES

All Shepherd University students, faculty, staff, and other parties with access to Shepherd University information assets and IT resources shall be responsible for:

USERS

- Usage of all information assets and IT resources in compliance with all applicable laws and Shepherd University policies, standards, guidelines, regulations, and procedures.
- Physically secure and safeguard information assets and IT resources within the user's possession and control, including abiding with the safe handling of data.
- Understand and comply with the guidance provided by this policy, as well as applicable compliance programs, including but not limited to those relating to FERPA and GLBA.
- Promptly report any suspected violation of this policy, any security events, and/or incidents involving a suspected compromise of a user's account or IT resource to itworkorder@shepherd.edu.

CIO/CISO – INFORMATION PRIVACY OFFICER

- Administer this policy.
- Ensure all requests to access or disclose information per policy is reasonably required in order to protect Shepherd University interests, is properly authorized, and meets the scope and conditions of permitted access.

- Provide authorization and direction to IT Services staff in accordance with this policy.
- Develops awareness and necessary training materials as they pertain to this policy.

IT SERVICES STAFF

- With appropriate authorization, take directed action in accordance with this policy to preserve, secure, and protect the interests of Shepherd University.
- Ensure all associated procedures are followed and documented accordingly when taking any actions outlined in this policy.

RELATED TOOLS

TRAINING

- Family Educational Rights & Privacy Act (FERPA) Training
- Gramm-Leach-Bliley Act (GLBA) Training

RELATED POLICIES & GUIDELINES

BOG#35: Information Technology Security
E-mail Policy
IT Information Security & Privacy Policy
International Travel Security Policy
Password Guidelines
Social Security Number Guidelines
Work from Home / Remote Access Guidelines

RELATED LAWS

- (DMCA) The Digital Millennium Copyright Act
- (FERPA) Family Educational Rights & Privacy Act
- (GLBA) Gramm-Leach-Bliley Act

POLICY: Acceptable Use Policy
IMPACT: Data, Technology, and IT Resources
RESPONSIBLE OFFICE: IT Services
CREATED: February, 11, 2010
REVIEWED: June 23, 2025, February 19, 2024; November 28, 2022; August 6, 2021

APPROVED BY: VP for Finance and Administration
VERSION: 25.1