Status Draft PolicyStat ID 21625549

UNIVERSITY OF WEST GEORGIA

| | |
|---|---|
| Last Approved | N/A |
| Effective | N/A |
| Next Review | N/A |
| Area | IT/ Management (Procedures) |
| Responsible Party | Information Technology Services |

# Acceptable Use for Computers and Network

Authority for Procedure granted by UWG PL #5001, Technology Use.

All University-owned, leased, managed, or otherwise authorized computing devices, network resources, and wireless communication resources are state assets and must be used in accordance with applicable laws, University System of Georgia (USG) Board of Regents (BOR) policies, University policies, and this procedure.

The purpose of this procedure is to establish standards for the acceptable use of University Technology Resources, support the University's mission of education, research, and service, and protect University Data assets from misuse, including Sensitive Data, from misuse, Unauthorized Access, and security threats.

**Note:** *Use of University Technology Resources constitutes acknowledgment of and responsibility for complying with this procedure.*

# A. Scope

This procedure applies to:

- All Authorized Users of University Technology Resources.
- Any University-owned device (i.e., computers, laptops, servers, printers, mobile devices, and other equipment) connected to or that transmits data over University networks.
- Any Personally Owned Device that accesses, stores, processes, transmits, or connects to University information resources or networks.
- Any Technology Resource owned, leased, rented, licensed, managed, or otherwise controlled or maintained by the University.

# B. Acceptable Use

Acceptable use of University Technology Resources include activities that support the University's


Copyright © 2026 University of West Georgia

mission and comply with federal and state laws, BOR policies, University policies, contractual obligations, and cybersecurity requirements. Authorized Users should access only the information they need for their University role.

# C. Prohibited and Inappropriate Use

Use of University Technology Resources for University business may be considered acceptable unless the user engages in prohibited activities including, but not limited to:

1. Harassment, discriminating against, intimidating, threatening, or retaliating against an individual or group, whether direct or indirect. (see UWG PL #4002 Non-Discrimination and Anti-Harassment).
2. Intentionally, recklessly, or negligently introducing, transmitting, or executing malware, ransomware, viruses, spyware, or other malicious code on University systems or networks.
3. Downloading, copying, storing, posting, transmitting, or distributing material that is illegal, proprietary, in violation of contractual obligations, or otherwise damaging to the University or individuals.
4. Accessing, attempting to access, or facilitating unauthorized access to systems, applications, services, data, or networks.
5. Scanning or testing University systems or networks for security weaknesses without written approval from the CIO or designee.
6. Sharing passwords, authentication credentials, access tokens, or user accounts unless expressly authorized.
7. Disabling, bypassing, interfering with, or attempting to circumvent cybersecurity controls, monitoring systems, security software, or access restrictions.
8. Hosting or operating technology services, applications, servers, cloud-based systems, file-sharing platforms, or network services without authorization from ITS.
9. Using University technology resources to disrupt or damage the academic, research, administrative, or business functions of the University or individuals.
10. Invading or threatening the privacy of an individual, including accessing, collecting, monitoring, disclosing, or distributing personal information without a legitimate educational, research, administrative, or business purpose.
11. Using University technology resources for personal commercial ventures, private consulting, non-University business activities, solicitation, fundraising, or advertising except as authorized by University policy or applicable law.
12. Violating any federal or state law, BOR policy, University policy, contractual agreement, software license, or copyright requirements.
13. Installing, copying, or using software or programs without proper licensing, authorization, or approval.
14. Engaging in phishing, spoofing, impersonation, social engineering, or other deceptive practices intended to gain unauthorized access to systems or information.
15. Storing, processing, or transmitting Sensitive or University Data using unauthorized devices, applications, cloud services, or third-party platforms.


Copyright © 2026 University of West Georgia

16. Entering confidential, restricted, regulated, or Sensitive Data into artificial intelligence (AI) tools or services without University authorization (see UWG's Generative AI guidance).
17. Failing to comply with reasonable directives regarding technology use issued by supervisors, ITS personnel, or other authorized University officials.

# 1. Personal Use

Limited Incidental Personal Use of University Technology Resources is permitted provided such use:

- Does not interfere with University operations or responsibilities;
- Does not incur significant costs to the University;
- Does not consume excessive Technology Resources;
- Does not compromise information security;
- Does not violate federal or state law, BOR policy, or University policy; and
- Does not interfere or conflict with academic, employment, or administrative responsibilities.

Incidental Personal Use remains subject to all requirements of this procedure.

# 2. User Responsibilities

Users must:

a. Complete required security awareness training;
b. Use multi-factor authentication (MFA) when required;
c. Never approve a sign-in request they did not initiate;
d. Lock or log off devices when left unattended; and
e. Delete or dispose of University Data in accordance with the USG Records Retention Schedules, UWG Records Information Management (RIM) Policy and associated procedures, and only through methods approved by ITS.

# D. Reporting Requirements

Users must immediately report known or suspected violations of this procedure to a supervisor, the Chief Information Officer (CIO), Information Technology Services (ITS), or the UWG Ethics and Compliance Reporting Hotline.

Users must also promptly report:

- Suspected cybersecurity incidents;
- Unauthorized Access to systems or data;
- Phishing attempts;
- Lost or stolen devices containing University Data;
- Malware infections;
- Unauthorized disclosures of Sensitive Data; and


Copyright © 2026 University of West Georgia

- Other technology-related security concerns.

Users should not try to investigate or fix a security problem on their own. They should report it and follow ITS instructions. Reporting an honest mistake, such as clicking a phishing link, will not by itself be treated as a violation.

The CIO or designee will take appropriate actions to protect University Technology Resources and information assets. When appropriate, the University's disciplinary or law enforcement authorities may coordinate with the CIO to investigate and respond to alleged violations.

Alleged violations will be addressed through applicable University disciplinary processes, including those found in the Employee Handbook, Faculty Handbook, Student Handbook and Wolf Code of Conduct, and other applicable policies and procedures.

# E. Monitoring and Privacy

University Technology Resources are owned by the University and provided primarily for conducting University business. While the University respects user privacy in accordance with applicable USG and UWG policies and legal requirements, users should have no expectation of privacy when using University Technology Resources, including but not limited to computers, networks, email systems, applications, cloud services, and telecommunications systems, except as otherwise provided by law.

The University may access, monitor, collect, review, preserve, and disclose information, communications, and associated metadata stored on or transmitted through these resources for legitimate business, operational, security, compliance, administrative, investigative, or legal purposes, or as required by applicable law, court order, public records obligations, or other legal processes.

By using University Technology Resources, users acknowledge and accept responsibility for complying with this procedure.

# F. Compliance and Enforcement

The CIO, Information Security Officer, ITS, and other authorized University officials may suspend, restrict, or terminate access to technology resources when necessary to protect University operations, security, or compliance obligations.

Failure to comply with this procedure may result in disciplinary action, loss of technology access privileges, referral to law enforcement, or other corrective actions as permitted by law and University policy.

Penalties may include:

- Suspension of University computing privileges;
- Disconnection of devices from University networks;
- Suspension from the University;
- Expulsion from the University;
- Termination of employment;
- Criminal prosecution where applicable;


Copyright © 2026 University of West Georgia

- Civil liability, where applicable; and
- Other disciplinary actions permitted by applicable police or law.

# G. Public Records

Information created, stored, received, transmitted, or maintained using University Technology Resources may constitute a public record and may be subject to disclosure pursuant to the Georgia Open Records Act O.C.G.A. §§ 50-18-70 et seq., subject to applicable legal exemptions, confidentiality requirements, and records retention obligations.

# Definitions

**Authorized User -** Any individual granted permission to access or use University technology resources, including faculty, staff, students, contractors, vendors, affiliates, volunteers, and guests.

**Artificial Intelligence (AI) Tool or Service -** Any software application, platform, or service that uses artificial intelligence technologies to generate, analyze, process, summarize, or otherwise manipulate data or content. **Examples:** Microsoft Copilot, ChatGPT, Google Gemini, Claude, Grammarly AI, image-generation tools, transcription services, Integrated AI, and AI-powered data analysis platforms. This includes AI features built into other software, such as Microsoft 365 or Zoom and other institutionally used technologies.

**Incidental Personal Use -** Limited personal use of University technology resources that does not interfere with University operations, create significant costs, consume excessive resources, compromise security, or violate applicable laws or University policies.

**Malware -** Malicious software or code intended to disrupt operations, gain unauthorized access, compromise data, or damage systems. **Examples:** Viruses, ransomware, spyware, trojans, keyloggers, malicious scripts, and similar threats.

**Personally Owned Device -** A device not owned by the University but used to access, store, process, transmit, or receive University information or connect to University technology resources.

**Sensitive Data -** University information classified as Personal, Public, Sensitive, Restricted, or otherwise requiring special safeguards because of legal, regulatory, contractual, operational, or privacy requirements. **Examples:** Student education records (FERPA), protected health information, financial records, employee personnel information, Social Security numbers, payment card information, passwords, research data subject to contractual restrictions, etc.

**Technology Resources -** University-owned, leased, licensed, managed, or authorized computers, mobile devices, software, applications, databases, cloud services, networks, email systems, communication systems, storage systems, and related information technology services.

Technology resources include, but are not limited to:

- Desktop computers, laptops, tablets, smartphones, printers, scanners, and servers;
- Wired and wireless networks, internet services, VPNs, and telecommunications systems;
- Email systems, messaging platforms, videoconferencing tools, and collaboration platforms;


Copyright © 2026 University of West Georgia

- Enterprise applications, databases, software, and cloud-based services;
- Learning management systems and academic technology platforms;
- Data storage systems, backup systems, and file-sharing services;
- Cybersecurity tools, identity and access management systems, and monitoring systems; and
- University-owned, licensed, or authorized digital information and data.

**Examples:** Microsoft 365, Outlook, Teams, OneDrive, Banner, Wolf Connect, campus Wi-Fi, University servers, shared drives, Zoom, cloud storage services, and University-managed databases.

**Unauthorized Access -** Accessing, attempting to access, using, sharing, altering, disclosing, or facilitating access to information, systems, applications, services, or networks without appropriate authorization, including going beyond the access a user has been given.

**University Data -** Any information created, received, collected, maintained, stored, transmitted, or otherwise managed by the University in support of its educational, research, administrative, operational, or business functions.

# Guidelines and Related materials

- **University System of Georgia (USG)**
  - USG Information Technology Handbook (ITHB)
  - USG Business Procedures Manual, Section 12.0 Data Governance and Management
  - USG PeachNet Acceptable Use Policy
- **UWG PolicyStat Library**
  - Cybersecurity Awareness Training Procedure
  - Intellectual Property Policy and associated procedures
  - Non-Discrimination and Anti-Harassment (NDAH) procedure
  - Records Information Management Policy and associated procedures
- UWG Generative Artificial Intelligence advisory webpage

## Approval Signatures

| Step Description | Approver | Date |
|---|---|---|


Copyright © 2026 University of West Georgia