

~~Acceptable Use of University Information Resources and Ethical Use of University Information Technology~~

Standards of Conduct – Expectations

CWU Policy 701-07

Effective: ~~June 1, 2005~~

Policy Review Date: YEAR

Policy Executive: Provost and Executive Vice President for Academic Affairs

Responsible Office/Unit: Information Services and Security

Policy Statement:

Information Assets and a trusted and effective information technology (IT) environment are vital to the Central Washington University (University) ongoing mission of discovery, learning and engagement. In furtherance of this mission, the University makes Information Assets and IT Resources available to:

- Support scholarship, research and instructional activities of university faculty,
- Facilitate the operations of the University,
- Provide access to university services and,
- Support student and campus life activities.

Applicability:

This policy applies to students, faculty and staff of the University and to all other persons accessing University IT Resources or Information Assets stored on or accessible via those resources, regardless of whether such resources or assets are accessed from on-campus or off-campus locations or via Devices (generally referred to in this policy as “users”).

Content:

Policy

- ~~(1) All university faculty, administrators, staff, and students, by virtue of their use of Central Washington University information technology resources, accept the responsibility of using these resources only for appropriate university activities. Library public computers are primarily intended for research.~~
- ~~(2) This policy covers all information technology resources that provide the Central Washington University community with computing, networking, telephony, and television/video resources.~~
 - ~~A. Information technology resources provide the Central Washington University community with access to local, national, and international information as well as the ability to communicate with other users worldwide. Information technology resources should be used in an acceptable and~~

ethical manner. For the benefit of the community, users must assume responsibility in the use of information technology resources. Use of information technology resources is governed by the United States Code, the laws of the state of Washington and Central Washington University policies. Some appropriate laws are listed at the end of this policy.

(3) Authorized Access

- A. Members of the Central Washington University community are authorized to use information technology resources provided by Central Washington University. The Central Washington University Library provides public computers with access to the internet.

(4) Acceptable Uses

- A. Information technology resources can be used for activities that support the mission of the university: learning, teaching, research, and university business.

(5) CWU Data Network Connection Policy

- A. Devices which extend the network such as but not limited to hubs, switches, bridges, routers and access points or computers functioning as such may not be connected to the CWU data network. Such devices are connected by the Networks and Operations department within Information Technology Services only. Users (students, faculty, and staff) may connect computers and printers to the CWU network.

(6) Legal Use Guidelines

- A. Information technology resources may not be used for any illegal or criminal purposes.
- B. Software, images, music or other intellectual property may only be used in compliance with the Copyright Act of 1976, amended 1994 and CWU Copyrights and Royalties Policy.
- C. Transmitting images, sounds, or messages to others which might reasonably to be considered harassing and/or malicious is not permissible.
- D. Using Central Washington University information technology resources to attempt to break into, gain root access, probe, disrupt, or obstruct any system is not permissible. Installation of invasive software or testing security flaws without authorization on any system is not permissible.
- E. Information technology resource use is subject to Use of State Resources WAC 292-110-010.

(7) Responsible and Ethical Use Guidelines

- A. Respect the intended use of all information technology resources for learning, teaching research, and university business purposes.
- B. Respect other users by not sending unwanted e-mail messages, maligning address information, flooding the system, sending frivolous messages, forging subscriptions, or tampering with accounts, files, or data that are not owned by your account.

- ~~C. Use only the user identification assigned to you, use it for the purposes for which it was intended, and do not share it with others.~~
- ~~D. Be sensitive to the public nature of shared resources, i.e. labs, modem pool, and disk space.~~
- ~~E. Occasional unsolicited receipt of e-mail should be deleted. Report repeated unsolicited receipt of e-mail as directed under Misuse of Information Technology Resources.~~
- ~~F. Student use of e-mail services is regulated by the Statement of Agreement between Central Washington University and the ASCWU Board of Directors which states, "The Associated Students of Central Washington University recognize all use of e-mail and internet services that is legal, adheres to University policy, and meets contractual obligations, as educational in nature."~~

(8) Reporting Misuse of Information Technology Resources

- ~~A. Complaints regarding misuse of information technology resources should be reported as indicated below.~~
- ~~B. Misuse of computing, networks, and telephony resources should be reported to Computing and Telecommunication Services.~~
- ~~C. Misuse of television/video resources should be reported to Media Circulation.~~

(9) Computing and Telecommunication Services Responsibilities

- ~~A. Computing and Telecommunication Services is responsible for insuring that the university's computing, networking, and telephony resources are properly used and protected by maintaining the integrity, security, and privacy of the resources and of users' electronic files, mail, records, and activities.~~

(10) Media Circulation Responsibilities

- ~~A. Media Circulation is responsible for ensuring that the university's video collection is properly used and protected.~~

(11) Investigations

- ~~A. Security measures are in place to assist with investigations of illegal and criminal activities or policy violations. Investigations performed by Computing and Telecommunication Services and Instructional Media Center are performed as appropriate and necessary.~~
- ~~B. If suspicion of misuse of information technology resources is found, the following steps will be taken to protect information technology resources and the user community:~~
 - ~~1. Computing, networking, and telephony accounts will be immediately suspended pending the outcome of any investigation.~~
 - ~~2. Files, data, usage logs, etc., will be inspected for evidence.~~

~~3. The violation will be reported to the appropriate authorities:~~

~~a. University policy violation to Student Affairs, the appropriate instructors, department chair, direct supervisor, vice presidents, or Auditing and Control.~~

~~b. Legal violations to the Campus Police, the FBI, the Secret Service, Human Rights, Auditing and Control, or the Attorney General's Office.~~

~~C. Violations of this policy will result in revocation of access to information technology resources as well as university disciplinary and/or legal action.~~

~~D. Violators are subject to any and all of the following:~~

~~1. Loss of information technology resources access.~~

~~2. University disciplinary actions (as prescribed in the Student Judicial Code, Faculty Code, WAC 357-40 for Civil Service, or Exempt Employees' Code).~~

~~3. Civil proceedings~~

~~4. Criminal prosecution~~

(12) — United States Code

~~A. Copyright Act of 1976, amended 1994 (Cornell Legal Information Institute)~~

~~B. Computer Fraud and Abuse Act of 1986 — 18 USC 1030 (Cornell Legal Information Institute)~~

~~C. Electronic Communications Privacy Act (Cornell Legal Information Institute)~~

~~D. Privacy — Electronic Communications Privacy Act — 18 USC 2701 (Cornell Legal Information Institute)~~

~~E. Unlawful access to stored communications — 18 USC Sec. 2701 (Cornell Legal Information Institute)~~

~~F. The Privacy Protection Act of 1980 — 42 USC Sec. 2000 aa (Cornell Legal Information Institute)~~

~~G. Public Telecommunications Act of 1992 — Telegraphs, Telephones, and radiotelegraphs 47 USC Sec. 605 (Cornell Legal Information Institute)~~

~~H. Interstate Transportation of Stolen Property Act —~~

(13) — Revised Code of Washington (RCW)

~~A. Computer Trespass — RCW 9A.52.110~~

~~B. Malicious mischief — RCW 9A.48.100~~

~~C. Use of state property — RCW 42.52.160~~

~~D. Theft of Telecommunication services — RCW 9A.56.262~~

~~(14) — Washington Administrative Code (WAC)~~

~~A. Use of state resources — WAC 292-110-010~~

~~B. Student Conduct Code — WAC 105-125~~

~~(15) — University Policies~~

~~A. Copyrights and Royalties Policy~~

~~B. Copyright for Computer Programs~~

~~C. Faculty Code of Personnel Policy and Procedure~~

~~(16) — Other~~

~~A. Licenses for Computer Software~~

(1) Appropriate Use

A. The University's Information Assets and IT Resources are provided for university-related purposes. Access to and usage of them entails certain expectations and responsibilities for all users, including managers of the University's IT environment. This policy sets forth those expectations and responsibilities.

B. Users residing in University housing are permitted to use the Residential Network (ResNet) for personal use and enjoyment in accordance with their housing agreement. The University does not routinely monitor ResNet activity for personal use. However, all users — including residential students — remain subject to applicable local, state, and federal laws, as well as restrictions on illegal activity and unauthorized commercial use.

C. Any use of Information Assets and IT Resources must be limited to the University-related purposes described in the Policy Statement.

D. Incidental and non-recurring (de minimis) personal use of IT Resources is allowed as part of the daily learning and work of all members of the University community, provided that such use does not violate any other applicable law, University policy, procedure, standard or regulation. Residents in University housing are exempt from this de minimis restriction.

E. Information Assets and IT Resources may not be used for private commercial activities that are not approved by the university, or for personal private gain.

F. The University accepts no responsibility to maintain or secure information related to personal use that a community member chooses to store on the University's IT Resources. The user accepts all risks associated with personal use.

G. 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

Commented [TP1]: Added by Policy Writer after feedback from UPAC

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Commented [TP2]: Added by Policy Writer after feedback from UPAC

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Font: 11 pt, Font color: Black, Highlight

2. Agrees to comply with all terms and conditions detailed within this policy.

H. The following uses of IT Resources are prohibited:

1. Sharing of login credentials
2. Attempted or successful circumvention of any technical, administrative, or physical safeguard implemented by the University or another entity
3. Intentional use, distribution or creation of viruses, worms, malicious software or keylogging techniques
4. Distributed denial of service practices or any other Device, program or practice of malicious motive
5. Connection of unauthorized networking devices (e.g., routers, switches, access points) to the university network without prior approval from CWU Information Services.
6. Sending of mass emails to individual Users, except for official university business. Emails to large groups will be sent using Distribution Lists or a university-approved mass mailing service.
7. Unauthorized use, copying or distribution of licensed software or copyrighted material.
8. Use of unlicensed, trial or open-source software unless: such use has been approved in advance by Information Services.
 - a. Such use has been approved in advance by Information Services; or
 - b. The software is used for academic, research, or instructional purposes from an established, reputable open-source repository and does not introduce unacceptable security risks; or
 - c. The software is used for personal purposes by students on the Residential Network.
9. Representing the University online without authorization.
10. Use of personal cloud or email services (e.g., personal Google accounts) to store university data.
11. Accessing Information Assets 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.
12. Accessing Information Assets or IT Resources in a manner designed to circumvent access limitations on confidential information without permission.
13. Use of IT Resources for organized political campaign activity on behalf of external political entities (e.g., national, state, or local campaigns), except where such use is part of authorized academic, research, or officially recognized University activities. This restriction does not apply to student governance or recognized student organization activities.

Commented [TP3]: Added by Policy Writer after feedback from UPAC

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Font: 11 pt, Font color: Black, Highlight

Commented [TP4]: Deleted by Policy Writer after feedback from UPAC

Formatted: Strikethrough, Highlight

Formatted: Strikethrough, Highlight

Formatted: Strikethrough, Highlight

Formatted: Highlight

Commented [TP5]: Added by Policy Writer after feedback from UPAC

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Font: 11 pt, Font color: Black

Formatted: Font: 11 pt, Font color: Black

14. Use of IT Resources that disable other IT Resources, consumes disproportionate IT Resources so that other users are denied reasonable access to those resources or materially increases the costs of IT Resources.
15. Use of IT Resources that violates any local, state or federal law or regulation or any University policy, procedure, standard or regulation.
16. Use of Information Assets or IT Resources for any purpose that could lead directly or indirectly to financial conflicts of interest, unless such use has been approved in advance in accordance with University policies. Any approval of the use of IT Resources under such policies is at the sole discretion of the University and must:
- a. Comply with all University software licenses and other intellectual property agreements,
 - b. Comply with all University policies, standards and procedures,
 - c. Comply with federal and state laws and regulations,
 - d. Not generate additional costs to the University and
 - e. Not interfere with university work or use of IT Resources.
- H. Use of University IT Resources is a privilege, not a right. Individuals assigned to an IT Resource account are responsible for all activity conducted under that account. Violations of this policy may result in the suspension, limitation or revocation of IT Resource privileges.
- I. Individuals with access that has been restricted should contact the IS Service Desk for details and resolution methods.

(2) Privacy, Operations and Monitoring

- A. The University recognizes that the right to privacy is a deeply held conviction, especially within intellectual and academic communities. Privacy is critical to the intellectual freedom that forms the foundation of higher education. However, a user's right to individual privacy in the context of the availability and use of IT Resources must be balanced with the University's legal obligations, the larger needs of the community, and the University's own Interests.
- B. The normal operation and maintenance of the University's IT Resources require backup and caching of Data and communications, the logging of activity, monitoring of general usage patterns and other such activities.
- C. The University may without notice to users, take any other action it deems necessary to preserve, protect and promote the Interests of the University. Where feasible and not otherwise precluded by law, active investigation, or third-party obligation, the University will endeavor to notify affected users as soon as reasonably practicable.
1. Such actions include, but are not limited to, those listed below pursuant to procedures or standards promulgated under the Information Security and Privacy Program.
- a. Intercept, access, scan, inspect, monitor, record, copy, store, use, disclose or sanitize the contents of any electronically stored Data employing IT Resources or any

Commented [TP6]: Added by Policy Writer after feedback from UPAC

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Font: 11 pt, Font color: Black, Highlight

communications or transmissions to or from IT Resources, whether via computer accounts, Devices or other means.

- b. Block unauthorized access to, and unauthorized uses of, the IT Resources and Information Assets.

D. The University seeks to maintain its IT environment and manage its Information Assets and IT Resources in a manner that respects individual privacy and promotes user trust. However, users should have no expectation of privacy beyond what is defined by policy or law.

E. University personnel do not routinely monitor the content of communications or transmissions using IT Resources, however, the Assistant Vice President of Information Services and Security (AVP/CIO) may authorize University technicians or administrators to take any of the actions described in Section (2).C.

1. The decision to take direct action will be based on one or more of the following:

- a. A reasonable belief that a process active in the account or Device is causing or may cause significant damage to University IT Resources or could cause loss/damage to the user, the University or third-party Data.
- b. A need to comply with a written request from federal, state or local law enforcement agencies and compliance with applicable University policies relating to the handling of such a request.
- c. Authorization by an appropriate order of a court of competent jurisdiction and compliance with applicable University policies related to the handling of such orders.
- d. A reasonable belief that an individual has violated or is violating University policies, standards, regulations or procedures using the accounts or Devices in question.
- e. A determination that a staff member, faculty member or student is deceased, has been terminated or is otherwise unavailable for the purpose of retrieving information that is critical to the operation of the unit in question.
- f. Receipt of a written request from the Office of the President or the Office of the Provost/Executive Vice President of Academic Affairs on behalf of the parents, guardian or personal representative of the estate of a deceased student.
- g. Receipt of a written Internal Audit request.
- h. A requirement to take action to comply with applicable law, and/or
- i. A determination by the AVP/CIO that access is necessary to preserve, protect or promote University Interests.

F. Without limiting its right to take action, the University may, in its sole discretion, disclose the results of any general or individual monitoring or access permitted by this policy and not prohibited by other contractual agreements, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies or use those results in appropriate University disciplinary proceedings.

G. Where applicable and warranted, the account or equipment user will be notified of the access or monitoring and the corrective actions taken.

H. In addition, and without violating federal, state or local laws, the University may use Business Administrative Data or Institutional Academic Data in the collection, analysis and reporting of metrics designed to fulfill the University's mission of discovery, learning and engagement; to advance its strategic objectives; and to preserve, protect and promote its Interests.

(3) Scope

A. As a general matter, the following types of Data are created or transmitted by, maintained on or accessed via IT Resources, and this policy applies to all such Data:

1. Information Assets stored in IT Resources, including computer accounts on University owned systems or other University owned Devices.
2. Information Assets stored in computer accounts or other Devices managed or hosted by trusted partners or third parties on behalf of the University, including but not limited to Cloud Computing Services or Hosting Services.
3. Voice and Data telecommunications traffic to, from or between University IT Resources and any University-owned Device, and traffic on personally owned Devices while using or accessing University IT Resources.

(4) Exclusions

A. Nothing in this policy changes or supersedes individuals' or the University's rights or obligations to comply with applicable federal and state laws or regulations governing the use and privacy of information, including:

1. Family Educational Rights and Privacy Act (FERPA),
2. Gramm-Leach- Bliley Act (GLBA),
3. Health Insurance Portability and Accountability Act of 1996 (HIPAA), and
4. Payment Card Industry Data Security Standard (PCI-DSS).

(5) Responsibilities

A. University faculty, staff and students, and other parties with access to University information assets and IT Resources have a responsibility to:

1. Use IT Resources in compliance with all applicable laws and University policies, standards, regulations and procedures.
2. Be familiar with and consult security standards and technical reference materials as applicable to the user's particular use of Information Assets and IT Resources.
3. Ensure multifactor authentication is configured and active with current methods on their account.

4. Use only CWU-approved systems for university data and understand related backup and retention rules.
5. Physically secure and safeguard IT Resources within the user's possession and control.
6. Use only IS-approved, supported, and up-to-date software on university owned systems.
7. 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, GLBA, HIPAA and PCI-DSS.
8. Report promptly to security@cwu.edu any suspected violation of this policy, any suspected IT security event, and any incident involving a suspected compromise of a user's University-provided account or Device.

B. Chief Information Security Officer (CISO) has a responsibility to:

1. Administer this policy.
2. Ensure any request to access or disclose information, per this policy, is reasonably required to protect University interest and is properly authorized.
3. Provide authorization and direction to technicians and administrators in accordance with this policy.

C. University-Authorized Technicians or Administrators have a responsibility to:

1. With appropriate authorization, take directed action in accordance with this policy to preserve, protect and promote the Interests of the University.
2. Ensure all associated procedures are followed when taking any action outlined in this policy.

(6) Exceptions

- A. Any request for an exception to this policy must be submitted in writing to security@cwu.edu.
- B. All exceptions require formal review and written approval from the Chief Information Officer (CIO) before any deviation from the policy may occur.

(7) References

- A. <https://watech.wa.gov/policies/non-agency-issued-device-security-standard>

(8) Definitions

- A. **Cloud Computing Services or Hosting Services:** Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) or other similar services by which providers deliver software applications or platforms for development to business clients via the Web or host and/or manage hardware that commonly supports data center operations.

B. Commercial Activities:

Economic activities geared toward a mass or specialized market and ordinarily intended to result in profit, and that are not part of one's university responsibilities. Commercial activities do not include the use of information technology resources for one-time, minimal transactions, such as students using their university email accounts to communicate with potential buyers for used textbooks. This type of transaction is considered incidental personal use.

C. Data:

Discrete, objective facts, statistics or other information collected or captured for reference, analysis, calculation, measurement or some other use.

D. Device(s):

Any mechanism used to store, retrieve, manipulate or transfer Data, including but not limited to a desktop or laptop computer, CD, USB flash drive, external USB hard drive, tablet, or smart phone.

E. Information Asset:

A body of contextualized or definable Data, regardless of format, having a recognizable and manageable value, risk, content and lifecycle and is generally defined, classified and managed by the University so that it can be understood, shared, protected and used effectively. In the ordinary course of its activities, the University regularly creates, collects, maintains, uses and transmits Information Assets.

F. Institutional Academic Data:

Information Assets that are created, collected, maintained, used, transmitted or otherwise processed by the University in connection with its mission of discovery and learning, including but not limited to general Data regarding student diversity, enrollment, academic performance, retention, majors and instructional activity; faculty and staff headcount and funding Data; research Data; and peer benchmarking Data.

G. Interests:

As used in this policy, the Interests of the University include, without limitation, those in:

1. Maintaining the stability, security and operational effectiveness of IT Resources and the services provided through them,
2. Safeguarding the availability, integrity and confidentiality of Information Assets maintained on IT Resources,
3. Protecting University assets and resources, including but not limited to IT Resources,
4. Monitoring the progress of effectiveness of the university and identifying improvements to services or delivery of programs,
5. Ensuring compliance with university policies, procedures, standards or regulations,
6. Preserving and promoting the integrity and reputation of the University,
7. Safeguarding the property, rights and Data of third parties,
8. Complying with the University's own legal responsibilities,
9. Promoting and protecting public safety, and

Formatted: Font: 11 pt, Bold, Italic, Font color: Black

10. Preserving the University's legal rights.

H. IT Resources (or Information Technology Resources):

All tangible and intangible computing and network assets provided by the University or by authorized third parties, regardless of whether those resources or assets are accessed from on-campus or off-campus locations or via devices. Examples of such assets include, but are not limited to, hardware, software, wired and wireless network and voice telecommunications assets and related bandwidth (including electronic mail), mobile devices, electronic and hardcopy information resources, and printers.

I. Mass Email

An electronic message distributed simultaneously to a large number of recipients typically exceeding 200 recipients.

J. Personal Data

Information relating to an identified or identifiable individual that is stored on University IT Resources for personal purposes and is not created or maintained in connection with University business. The University accepts no responsibility to maintain or protect Personal Data stored on its IT Resources.

K. University Data (University Information)

Information created, received, maintained, or transmitted by or on behalf of CWU in connection with its mission, operations, or administration, including student records, employee records, research data, financial records, institutional communications, and course or instructional materials created by University employees in the performance of their university duties.

Formatted: Highlight

Commented [TP7]: Definitions added by Policy Writer after feedback from UPAC

Formatted: Highlight

Formatted: Highlight

History:

UCC: 5/16/97; Pres Cab: 9/8/97; Responsibility: Operations; Authority: Cabinet/UPAC; Reviewed/Endorsed by: Cabinet/UPAC; Review/Effective Date: 06/01/2005; Approved by: James L. Gaudino, President
Reformatted and Assigned new Policy Number - Previous Policy CWUP 2-40-010, June 2025
2-26-2026 – Housekeeping Change