SUBJECT:	Information Technology				
POLICY:	701.2 Computer and Network Usage				
PROCEDURE:					
EFFECTIVE:	November 2003	**REVISED:**	March 2023	**REVIEWED:**	

Introduction and Purpose

Great Falls College MSU provides computer systems, network access, internet services, software, technology equipment, and related information resources to support instruction, learning, student services, library services, administration, communication, research, public access, and college operations.

The purpose of this policy is to establish acceptable and responsible use requirements for Great Falls College MSU computing facilities, services, networks, devices, software, and information resources. This policy is intended to protect the confidentiality, integrity, availability, and appropriate use of college technology resources while supporting lawful, ethical, secure, and mission-related access.

This policy applies to all users of Great Falls College MSU computing and network resources, including students, faculty, staff, public guests, library patrons, vendors, contractors, volunteers, affiliates, and other individuals who access or use college technology resources.

Great Falls College MSU technology resources are provided for approved educational, business, administrative, public service, and mission-related purposes. Use of these resources is a privilege that carries responsibility.

~~INTRODUCTION AND PURPOSE~~

~~Great Falls College MSU is pleased to be able to offerstudents a wide variety of computer facilities, services, equipment, and software. Students are encouraged to use them within the guidelines. The Montana University System Board of Regents has implemented information technology policies that apply to all public institutions of higher education within the state of Montana. These policies may be reviewed at Section 1300-Information Technology.~~

~~Failure to comply with these guidelines may result in disciplinary action, including expulsion from the campus and criminal prosecution.~~

~~POLICY~~

~~Access~~

~~Students have access to computers on the Great Falls College MSU' Campus at several locations – in computer labs, the library, computer classrooms, and at the computer kiosks outside the bookstore. Students currently enrolled for classes also may have access to wireless networking. By connecting to the wireless networks, students agree to comply with the Acceptable Use Policy and the Network Attached Device Policy and Standards. . Students and non-students are welcome to use the computer kiosks, but are asked to share that resource with others who wish to use it.~~

~~Because access to computer labs and classrooms is purchased by students through their computer fees, computer labs and classrooms may be used only by students currently enrolled in classes, workshops, or seminars at the College. Students are allowed access to open computer-equipped classrooms when the~~

~~building is open, Monday - Friday. On weekends, in the event of an overflow from the Library Computer Lab, a classroom may be unlocked for student use.~~

~~Privacy of Information~~

~~Great Falls College MSU campus computer systems and networks are public and subject to Montana State laws. Files of personal information, including programs, regardless of the medium on which they are stored or transmitted, may be considered public information and are stored on Great Falls College MSU's computers. However, simply being able to access a file or other information does not imply permission to do so. The preservation of individual privacy is given high regard on this Campus, and students may not use electronic and other technological methods to infringe upon another's privacy. No one should look at, copy, alter, or destroy any individual's personal files without explicit permission from that individual, unless authorized by the Dean of the College in compliance with law or regulation.~~

~~Libel, Slander, and Harassment~~

~~No member of the college community may, under any circumstances, use - Great Falls MSU's computers or networks to libel, slander, or harass any other person. Harassment includes intentionally using the computer to threaten or sexually harass another person; contact another person repeatedly regarding a matter for which one does not have a legal right to communicate once the recipient has provided reasonable notice that he or she desires such communication to cease; and/or disrupt or damage someone's academic, research, administrative, or related pursuits.~~

~~Responsible~~Roles, ~~Use~~Responsibilities, ~~of~~& ~~Resources~~Exceptions

Information Technology Services is the responsible office for administration, interpretation, implementation, and periodic review of this policy, in coordination with College leadership and applicable Montana University System Offices.

Any use, access, or activity that would otherwise violate this policy but is necessary for an approved instructional, research, security testing, or operational purpose must be requested in writing to Information Technology Services prior to the activity taking place, and must include a description, justification, scope, and duration.

An approved exception may be modified or revoked when conditions change or when the exception creates an unacceptable security, operational, legal, privacy, or compliance risk.

Outside work, compensated activity, or use benefiting an organization unrelated to Great Falls College MSU requires written permission from the Dean/CEO or designee, in addition to any technology-related exception.

Policy

All users must use Great Falls College MSU computing facilities, services, networks, systems, software, and technology equipment in a lawful, ethical, secure, respectful, and responsible manner.

Users must not use college technology resources in a way that:

Violates federal, state, local, Montana University System, Montana Board of Regents, MSU, or Great Falls College MSU policy.

Interferes with college operations, instruction, services, or network performance.

Compromises the security, privacy, availability, or integrity of college systems, data, or users.
Harasses, threatens, discriminates against, or harms another person.
Accesses, uses, copies, modifies, deletes, discloses, or distributes information without authorization.
Uses public resources in a way that prevents equitable access by others.
Uses state facilities or equipment for prohibited personal, commercial, political, or financial gain.
Information Technology Services may restrict, suspend, disable, monitor, quarantine, or remove access when necessary to protect college systems, data, users, technology resources, or operations. Such action may be taken immediately and without prior notice when risk is identified.

Scope

This policy applies to all users who access or use Great Falls College MSU technology resources, whether access occurs on campus, remotely, through wireless networks, through public computers, through personally owned devices, through college-owned devices, or through third-party systems connected to college resources.
This policy applies to, but is not limited to:
Desktop computers, laptops, tablets, mobile devices, kiosks, printers, scanners, phones, classroom technology, library computers, lab computers, and other technology equipment.
Wired and wireless networks, internet access, remote access, guest access, and cloud-connected services.
College accounts, email, learning systems, administrative systems, file storage, collaboration platforms, software, databases, and applications.
College-owned, personally owned, vendor-owned, contractor-owned, public-use, and temporary-use devices connected to or used with college technology resources.

Access and Eligibility

Great Falls College MSU provides access to technology resources based on user role, business need, instructional need, public service purpose, resource availability, security requirements, and applicable policy.
Students may have access to computers, software, wireless networking, learning systems, lab systems, library resources, and other technology services based on enrollment status, course participation, program requirements, and resource availability.
Faculty and staff may have access to computers, accounts, software, administrative systems, network services, and data necessary to perform assigned job duties and approved college functions.
Public guests and visitors may have limited access to designated public-use technology resources, guest wireless networks, kiosks, or other approved services. Guest access does not imply access to internal college systems, restricted data, employee resources, or student systems.
Library patrons may have access to designated library technology resources in accordance with library procedures, resource availability, licensing restrictions, security requirements, and applicable college policy.
Vendors, contractors, volunteers, and affiliates may access college technology resources only when authorized and only for the approved purpose, scope, and duration.

Access may be limited, denied, modified, monitored, or terminated based on security risk, resource availability, licensing requirements, operational need, changes in the user's institutional relationship, or an authorized administrative, employment, student-conduct, contractual, or legal action.

Responsible and Acceptable Use

Users are responsible for using college technology resources respectfully, securely, lawfully, and efficiently.
Acceptable use includes:
Instruction, learning, academic work, research, and student support.
College business, administration, communication, and public service.
Library access, public access, and guest access when provided for an approved purpose.
Authorized access to college systems, data, software, and services.
Limited incidental personal use when it does not interfere with college operations, violate policy or law, consume excessive resources, create security risk, or result in personal financial gain or prohibited activity, meaning brief, occasional use (for example, a short personal email or reference lookup) that does not exceed college-published resource thresholds for storage, bandwidth, or printing, and does not require installation of software or dedicated equipment.
Users must:
Use only accounts, systems, and resources they are authorized to access.
Protect passwords, passphrases, authentication methods, and account credentials.
Follow college instructions for secure use of technology resources.
Respect the privacy, work, files, communications, and rights of others.
Comply with software licenses, copyright requirements, data protection rules, and other applicable restrictions.
Share public-use resources fairly and yield resources when others need them for higher-priority academic, library, instructional, or college-related use.
Report suspected security incidents, compromised accounts, unauthorized access, malware, lost or stolen college devices, and other technology concerns to Information Technology Services as soon as reasonably possible.

Public, Guest, and Library Patron Use

Public guests and library patrons may use designated college technology resources when such access is provided by the college. Public or guest access may be limited by location, schedule, staffing, availability, system capability, licensing, security requirements, and priority of college operations.
Public-use resources may be subject to time limits, content restrictions, printing limits, bandwidth limits, authentication requirements, monitoring, filtering, or other controls necessary to support equitable use, security, legal compliance, and operational needs.
Use of public or library technology resources must not:
Interfere with students, faculty, staff, library patrons, or college operations.
Bypass computer, network, internet, or content restrictions.
Access or attempt to access restricted college systems or data.

Install software or change system settings.
Save confidential or sensitive personal information on public computers.
Use public computers for prohibited commercial, political, financial gain, harassing, unlawful, or disruptive activity.
Damage, disable, tamper with, or remove college technology equipment.
The college may end or restrict public, guest, or library patron access when necessary for security, availability, conduct, policy compliance, or operational reasons.

Privacy, Monitoring, and No Expectation of Privacy

Great Falls College MSU technology resources are college resources and may be subject to monitoring, logging, access review, security scanning, retention, disclosure, or inspection as permitted by applicable law, policy, Montana Board of Regents requirements, and operational need.
Monitoring may occur to:
Maintain system and network availability.
Troubleshoot technical issues.
Protect systems, data, users, and college operations.
Detect unauthorized access, malware, misuse, or policy violations.
~~Students are responsible for knowing what information resources (including networks) are available, remembering that the members of the college community share them, and refraining from all acts that waste these resources or prevent others from using them. Details regarding available resources can be obtained by consulting with the Information Technology Services Department.~~
~~Students are discouraged from using campus computing and network services for non-academic purposes such as game playing and non-academic chat rooms. A student using a computer for non- academic matters must give it up when someone who wishes to use the computer for academic purposes is waiting.~~
~~State law restricts the use of state facilities and equipment for personal gain or benefit. Computing facilities, services, and networks at Great Falls College MSU may not be used for compensated outside work or work for the benefit of organizations not related to Great Falls College MSU without written permission from the Dean/CEO. Electronic gambling, stock trading, or any other financial gain method conducted on college computers, services, or networks are forbidden. State law also restricts the use of college computer systems for political advocacy or for commercial advertising.~~
~~System~~Investigate ~~Security~~security incidents.
Support compliance, legal, public records, or administrative requirements.
Users should have no expectation of privacy when using college technology resources except as provided by applicable law, policy, or regulation.
Access to another person's files, communications, accounts, data, or activity is prohibited unless specifically authorized by the individual, by job responsibility, by Information Technology Services, by college leadership, or as otherwise permitted by law, policy, or regulation. Any such access, other than routine, role-based access performed in the ordinary course of assigned duties, requires written approval and a documented business justification, retained by Information Technology Services.

Legal and Public Records Requests

Information Technology Services will comply with valid subpoenas, court orders, public records requests, and law enforcement requests for data consistent with applicable law and college legal counsel review.
Users will be notified of a request involving their data only where required or permitted by law.

Protection of Information and Data

Great Falls College MSU classifies institutional data into four categories: Public, Internal, Confidential, and Restricted. Users must handle data according to its classification level, as defined in the Definitions section and any accompanying Data Classification Standard maintained by Information Technology Services.
Restricted data (including FERPA, HIPAA, financial account, and credential data) must be stored only in approved systems, encrypted at rest and in transit, and never stored on personally owned devices, public computers, or unapproved cloud services. Users uncertain of a data element's classification must treat it as Confidential until confirmed otherwise by Information Technology Services or the applicable data owner.
Users must protect institutional data and sensitive information, data classified as Internal, Confidential, or Restricted, from unauthorized access, disclosure, alteration, loss, or misuse.
Users must not:
Access data they do not have permission to use.
Share Restricted or Confidential information with unauthorized individuals.
Store Restricted or Confidential information in unauthorized locations.
Transmit Restricted or Confidential information through unapproved services.
Use public or shared computers to access sensitive systems unless authorized and appropriate safeguards are followed.
Leave active sessions unattended on shared, public, classroom, lab, library, or kiosk computers.
Attempt to bypass data protection, authentication, or access controls.
Faculty, staff, student employees, vendors, contractors, and other users with access to institutional data are responsible for following applicable data handling, retention, privacy, FERPA, HIPAA, financial, contractual, and institutional requirements.

Credentials and Account Security

Users are responsible for protecting their accounts and authentication credentials.
Users must not:
Share passwords, passphrases, multifactor authentication prompts, tokens, keys, or other credentials.
Allow another person to use their account.
Use another person’s account.
Attempt to obtain another person’s credentials.
Approve authentication prompts they did not initiate.
Store passwords in an insecure manner.
Bypass authentication, access controls, or account restrictions.
Accounts may be disabled, locked, reset, restricted, or reviewed when suspicious activity, compromise, misuse, or policy violation is suspected.

Prohibited Uses

The following uses of college technology resources are prohibited unless specifically authorized by Information Technology Services and applicable college leadership for a lawful and approved college purpose:

Attempting to gain unauthorized access to systems, accounts, data, networks, devices, or services.

Circumventing or attempting to circumvent security controls, authentication systems, network controls, filters, monitoring tools, or access restrictions.

Introducing, creating, distributing, or intentionally enabling malware, viruses, ransomware, worms, spyware, malicious code, or harmful tools.

Disrupting, degrading, overloading, scanning, probing, intercepting, or attacking systems, networks, services, or accounts.

Damaging, deleting, altering, copying, disclosing, or destroying files, software, configurations, equipment, or data without authorization.

Installing or using unauthorized software, services, tools, network devices, remote access tools, or administrative utilities.

Using college resources for harassment, threats, intimidation, doxing, stalking, bullying, discrimination, libel, slander, or other harmful conduct.

Viewing, storing, transmitting, or distributing unlawful content.

Violating copyright, licensing, intellectual property, or software use restrictions.

Using college systems to impersonate another person or misrepresent identity, affiliation, or authorization, including impersonation through AI-generated content.

Using public, guest, library, classroom, or lab systems for activity that prevents others from using them for approved academic, library, public service, or college-related purposes.

Using college resources to bypass security tools, content restrictions, or network segmentation.

Using college resources for unauthorized commercial activity, political advocacy, financial gain, gambling, advertising, or compensated outside work.

Use for Personal Gain, Commercial Activity, Political Advocacy, and Financial Activity

State law restricts the use of state facilities and equipment for personal gain or private benefit. Great Falls College MSU computing facilities, services, equipment, software, and networks may not be used for compensated outside work or for work benefiting organizations not related to Great Falls College MSU unless written permission has been granted by the Dean/CEO or designee.

College technology resources may not be used for electronic gambling, stock trading, cryptocurrency trading or mining, speculative trading, commercial advertising, unauthorized business activity, or any other method intended to produce personal financial gain or private benefit.

State law also restricts the use of college computer systems, equipment, services, and networks for political advocacy or commercial advertising. Users must not use college technology resources for political campaign activity, lobbying activity not authorized as part of official college duties, campaign communications, campaign fundraising, partisan advocacy, or commercial promotion unless such use is expressly permitted by law, policy, and written college authorization.

This section does not prohibit limited incidental personal use that is otherwise lawful, does not involve personal financial gain, does not interfere with college operations, does not consume excessive resources, and does not violate applicable law, policy, or college requirements.

Harassment, Threats, and Disruptive Conduct

No user may use Great Falls College MSU technology resources to harass, threaten, intimidate, bully, discriminate against, slander, libel, or otherwise harm another person.
Prohibited conduct includes, but is not limited to:
Threatening, abusive, intimidating, or harassing messages.
Repeated unwanted contact after a reasonable request to stop, as further defined in the college's Harassment and Title IX policies.
Use of technology to disrupt another person's academic, employment, library, public access, administrative, or college-related activities.
Unauthorized access to another person's accounts, files, records, or communications.
Use of college technology resources to target, embarrass, impersonate, exploit, or harm another person.
Conduct that may also violate student conduct policies, employee policies, anti-discrimination policies, harassment policies, public safety procedures, or law may be referred to the appropriate college office or external authority.

Software, Licensing, and Copyright

No software may be installed, copied, downloaded, executed, modified, removed, or used on college-owned or college-managed systems unless permitted by Information Technology Services, applicable licensing terms, and college procedure.
Users must comply with copyright law, software license agreements, database license agreements, publisher restrictions, library resource licenses, and other contractual requirements.
Users must not:
Install unauthorized software on college systems.
Use unlicensed or pirated software.
Copy or distribute software without authorization.
Disable licensing controls or security controls.
Use college systems to unlawfully download, share, stream, copy, or distribute copyrighted materials.
Modify college system configurations without authorization.
Public, library, classroom, lab, kiosk, and shared computers may be reset, restricted, monitored, or configured to prevent unauthorized software installation, data retention, or configuration changes.

System and Network Security

~~Students~~Users are prohibited from attempting to circumvent or subvert ~~any~~ security measures, degrade the performance of a computer system or network, or deprive authorized ~~personnel~~users of ~~resources or~~ access to ~~any~~ college ~~computer~~technology ~~system or network. The following harmful activities are also prohibited: creating or propagating viruses; disrupting services; deleting or damaging files without proper~~

~~authorization; intentionally destroying or damaging equipment, software, or data belonging to Great Falls College MSU or other users; and the like. No software may be installed, copied, or used on campus resources except as permitted by system administrators.~~resources.

Users must not:

Attempt unauthorized access to college or third-party systems.

Scan, probe, attack, intercept, or monitor network traffic without authorization.

Connect unauthorized devices, wireless access points, routers, switches, servers, or network services.

Disable endpoint protection, monitoring, logging, encryption, or security controls.

Share network access in an unauthorized manner.

Use tools intended to exploit, crack, bypass, or compromise systems unless specifically authorized for an approved college purpose.

Create, store, execute, test, or distribute malicious code or offensive security tools outside an approved instructional or security environment.

Intentionally disrupt services, damage equipment, or interfere with normal operations.

Information Technology Services may isolate, disconnect, restrict, remove, or inspect systems that present a security risk, violate policy, appear compromised, or interfere with network operations.

Artificial Intelligence Tools

Users may use college-approved artificial intelligence and generative AI tools for instructional, research, and administrative purposes consistent with academic integrity requirements and applicable course, program, or departmental guidelines.

Users must not:

Enter Confidential or Restricted data into any AI tool not reviewed and approved by Information Technology Services for that data type.

Rely on AI-generated output for official college records, legal, financial, or compliance purposes without human review and verification.

Use AI tools to generate content that violates this policy, including harassment, impersonation, or academic dishonesty.

Shared, Public, Lab, Classroom, and Library Computers

Shared computers are provided for approved academic, instructional, library, public access, and college-related purposes.

Users of shared computers must:

Sign out when finished.

Remove personal files when appropriate.

Avoid storing sensitive information on shared or public computers.

Yield resources when required by college, library, instructional, or operational priorities.

Follow posted rules, lab rules, library procedures, and staff instructions.

Avoid changing system settings, installing software, disabling controls, or attempting to bypass restrictions.

The college is not responsible for personal files, credentials, browser sessions, or personal information left on shared or public computers.

Resource Stewardship

College technology resources are shared resources. Users must use them responsibly and avoid activity that wastes resources, prevents others from using them, or interferes with college operations.
Information Technology Services may limit or restrict use that consumes bandwidth, storage, processing capacity, printing resources, licensing capacity, or support resources beyond baseline thresholds.
Non-college use may be restricted when academic, instructional, administrative, library, public service, or college operational needs require access.

Incident Reporting

Users must promptly report suspected or confirmed technology security concerns to Information Technology Services.
Reportable concerns include:
Lost or stolen college devices.
Compromised accounts.
Suspicious login activity.
Malware or ransomware.
Unauthorized access.
Unauthorized devices.
Data exposure.
Phishing.
System misuse.
Interference with technology resources.
Security control bypass attempts.
Users must cooperate with Information Technology Services and appropriate college officials during investigation, containment, remediation, and recovery activities.

Enforcement

Failure to comply with this policy may result in one or more of the following:
Warning or education.
Restriction, suspension, or removal of technology access.
Removal of unauthorized software or devices.
Device quarantine or disconnection.
Account lockout, password reset, or access review.
Referral to student conduct processes.
Referral to employee disciplinary processes.
Referral to library, facilities, or public safety procedures.
Contractual action for vendors or contractors.

Civil or criminal prosecution where appropriate.
Information Technology Services may take immediate action to protect systems, data, users, or operations when a device, account, activity, or user presents risk.

Definitions

For purposes of this policy, the following definitions apply:
Technology resources means college-owned, college-managed, college-provided, or college-authorized computing facilities, services, network access, systems, devices, software, accounts, data, and related information resources.
User means any individual who accesses or uses college technology resources, including students, faculty, staff, public guests, library patrons, vendors, contractors, volunteers, affiliates, and other authorized users.
Authorized use means use that is consistent with college policy, applicable law, user role, approved access, and the educational, administrative, public service, or business purpose for which the resource is provided.
Public-use technology means college technology resources made available for public, guest, visitor, library patron, kiosk, or other limited-use access.
Institutional data means data created, received, maintained, processed, stored, or transmitted by or on behalf of Great Falls College MSU.
Sensitive information means information that is protected by law, regulation, contract, policy, or institutional requirement, including but not limited to student records, employee information, financial information, credentials, security information, health-related information, and other confidential or restricted data.
Public data means information approved for public release with no restriction on disclosure.
Internal data means information intended for use within the college community that is not approved for public release.
Confidential data means information protected by policy, contract, or business requirement, including personnel records not classified as Restricted, budget and financial planning documents, and unpublished research.
Restricted data means information protected by law or regulation where unauthorized disclosure creates legal, financial, or reputational risk, including FERPA-protected student records, HIPAA-protected health information, Social Security numbers, financial account and payment card data, and login credentials or security configurations.

Reference

706.1 Data Stewardship
Enterprise Data Stewardship Policy - OneMSU Policy | Montana State University