



**President's**  
Policy Statement  
University Policy  
Library

Operational Area	Information and Technology
Responsible Executive	Chief Information Officer
Responsible Office	Information Technology Services
Effective	June 1, 2026

# Acceptable Use of Computing Systems Policy

## Information and Technology

### Contents:

- I. Introduction
- II. Roles and Responsibilities
- III. Policy Statement
- IV. Enforcement and Reporting
- V. Related Information
- VI. Policy History
- VII. Policy Approval

## I. INTRODUCTION

- A. **Authority:** C.R.S. § 23-54-102, et seq. (2026) authorizes the Trustees of Metropolitan State University of Denver (“MSU Denver” or “University”) to establish rules and regulations to govern and operate the University and its programs. The Board of Trustees (“Board” or “Trustees”) retain authority to approve, interpret, and administer policies pertaining to University governance. The Trustees authorize the President of MSU Denver to approve, administer, and interpret policies pertaining to University operations.
- B. **Purpose:** MSU Denver’s information security policies protect the University’s critical data and information systems from loss, damage, or unauthorized access or disclosure. This policy educates the University community on data protection, outlines procedures to safeguard the confidentiality, integrity, and availability of University data, and ensures compliance with applicable privacy and confidentiality regulations.
- C. **Scope:** This policy applies to all individuals with access to University data or information technology systems, including students, faculty, staff, and contractors. Contractors and other affiliated individuals must agree to follow the University’s information security policies before gaining access. When applicable, role-based policies and procedures will be provided to specific user groups based on functional requirements and data classification.



President's  
Policy Statement  
University Policy  
Library

Operational Area	Information and Technology
Responsible Executive	Chief Information Officer
Responsible Office	Information Technology Services
Effective	June 1, 2026

# Acceptable Use of Computing Systems Policy

## Information and Technology

### II. ROLES AND RESPONSIBILITIES

- A. **Responsible Executive:** Chief Information Officer
- B. **Responsible Administrator:** Chief Information Security Officer
- C. **Responsible Office:** Information Technology Services
- D. **Policy Contact:** IT Services, [Information Technology Services Webpage](#), 303-352-7000

### III. POLICY STATEMENT

The purpose of this policy is to ensure that all users of MSU Denver computing systems utilize these resources in a manner that supports the mission of the University and in a manner that protects these resources and their associated data from inappropriate access, usage, or other harm. All faculty, staff, students, contractors, and other users of University-owned and maintained computer equipment and network resources, must follow acceptable use policies.

- A. **Acceptable Use Standards:** Users of MSU Denver computing systems must apply standards of normal academic and professional ethics while utilizing computing systems resources. These standards are found in the [Student Code of Conduct](#) and [Faculty Employment Handbook](#).
- B. **Identification and Authentication:** Users of MSU Denver computing systems must utilize user IDs or other unique user identification when accessing computer and/or network resources. Individuals must not knowingly access systems using another person's account credentials, and users must not share or allow others (including automated tools, such as AI meeting assistants, AI browser plug-ins, or digital agents) to use their account credentials under any circumstances. Users must take reasonable precautions to protect their identity, passwords, and access to University computing systems. Misuse or negligent handling of credentials is subject to disciplinary action.
- C. **Personal Use:** MSU Denver computer systems may be accessed for incidental personal use, provided that such use does not result in noticeable impacts to system performance, incremental costs, or performance of employee duties. Users must not store personal, sensitive, or private information (e.g., personal tax records, estate documents, private correspondence) on institution systems. All data stored on University systems may be subject to access or review as



**President’s**  
Policy Statement  
University Policy  
Library

Operational Area	Information and Technology
Responsible Executive	Chief Information Officer
Responsible Office	Information Technology Services
Effective	June 1, 2026

## Acceptable Use of Computing Systems Policy

### Information and Technology

outlined in this policy. Users are strongly discouraged from using University accounts or storage for personal data unrelated to University business.

**D. Intellectual Property and Copyright:** Users of MSU Denver computing systems may only use legally licensed and obtained software in compliance with [University policies](#) and applicable copyright and intellectual property laws. MSU Denver is a member of EDUCAUSE, and users are expected to adhere to the Educause Code of Software and Intellectual Rights which states: (See [EDUCOM: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community/ITAA](#)):

1. “Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.”

**E. Privacy:** Computer users must respect the privacy of others by refraining from inspecting, disclosing, or modifying data without the consent of the individual or individuals involved, except as permitted as part of their employment, and then only to the extent necessary for employment. When an individual leaves, is terminated, or passes away, access to their data may be reassigned or examined to maintain institutional operations or meet legal requirements. After affiliation with the University ends, confidentiality of digital content may not be maintained.

**F. False Identity:** Users of University email or other electronic communications systems shall not employ a false identity, nor may e-mail be sent anonymously with the intent to deceive.

**G. Interference:**

1. University computing services shall not be used for purposes that cause, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted/unsolicited interference with others' use of Computing Systems and Services.



**President's**  
Policy Statement  
University Policy  
Library

Operational Area	Information and Technology
Responsible Executive	Chief Information Officer
Responsible Office	Information Technology Services
Effective	June 1, 2026

## Acceptable Use of Computing Systems Policy

### Information and Technology

2. This provision explicitly prohibits the posting of unsolicited electronic mail to lists of individuals, and the inclusion on electronic mail lists of individuals who have not requested membership on the lists.
  3. Students may be required to accept membership in an electronic mailing list for a class in which they are registered or for the purpose of official communications between authorized University personnel and an identified group of students.
  4. Faculty and staff may be required to accept membership in an electronic mailing list for the purpose of official University communications.
  5. The University may take action to protect computer users from interference. [Information Technology Services \(ITS\)](#) or someone designated by the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO) may authorize the termination of connections with internal or external systems or services which interfere with the operation of University computing systems.
- H. **Obscenity and Harassment:** University Computing Systems and Services may not be used in a manner that would violate University policies on [Prohibition of Discrimination, Harassment, Sexual Misconduct, Title IX Violations, and Retaliation](#). Links to the Student Code of Conduct and Faculty Handbook are provided below.
- I. **Enforcement:** Computer and network activity are monitored by automated systems and by authorized individuals for purposes of maintaining system performance and security. Files, logs, and systems will be scanned in response to monitoring system alerts for the purpose of identifying, evaluating and investigating risks from potential malware or compromise of systems and accounts. All data, programs, and files placed on or contained in the University computer systems are subject to the University's copyright, patent, and privacy policies.
- J. **Exceptions:** Adherence to Information Security Policies is mandatory and may be based on State or Federal statute, contract language, or information security standards. These policies are not intended to unreasonably interfere with system utilization. Individuals must contact the IT Services Help Desk to report security risks, violations of policy, or to make requests for exceptions or amendments to the policies. The Chief Information Security Officer (CISO) and other IT Services staff will respond to all reported security issues and will work with the policy subcommittee to allow for development of appropriate updates to policies. Violations of these policies may result in fitting administrative action up to and



Operational Area	Information and Technology
Responsible Executive	Chief Information Officer
Responsible Office	Information Technology Services
Effective	June 1, 2026

## Acceptable Use of Computing Systems Policy

### Information and Technology

including revocation of system privileges, employee termination, or student expulsion.

#### K. Sanctions:

1. Violation of University policies governing the use of University computing services may result in restriction or termination of access to University information technology resources. In addition, disciplinary action may be applicable under other University policies, guidelines, procedures, or collective bargaining agreements, up to and including dismissal.
2. In instances when individuals are suspected of abuse of computer usage, the contents of user files may also be inspected upon the approval of the [Office of General Counsel](#), in addition to one or more of the following offices: [Human Resources](#), [Office of Equal Opportunity](#), or the [Dean of Students](#). Any such monitoring or inspection must be formally requested and approved through [IT Services Helpdesk](#) tickets to ensure that the request and any related activities are appropriately documented.
3. At the discretion of the manager of the computer system or service in question, or designee, in collaboration with the appropriate authority, computer use privileges may be temporarily or permanently revoked pending the outcome of an investigation of misuse or finding of violation of this policy. When practical and appropriate, notice will be given in advance of revocation.

## IV. ENFORCEMENT AND REPORTING

- A. Adherence to MSU Denver information security policies is mandatory and may be based on state or federal statute, contract language, or information security standards. These policies are not intended to unreasonably interfere with system utilization.
- B. All users of University computing systems must review and acknowledge this Acceptable Use Policy (via Workday) on an annual basis. Acknowledgement will be tracked by Information Technology Services and is required for continued system access.
- C. Individuals must contact the IT Service Desk to report security risks, violations of policy, or to make requests for exceptions or amendments to the policies. The Chief Information Security Officer (CISO) and other IT Services staff will respond



Operational Area	Information and Technology
Responsible Executive	Chief Information Officer
Responsible Office	Information Technology Services
Effective	June 1, 2026

## Acceptable Use of Computing Systems Policy

### Information and Technology

- to all reported security issues and will work with the [University Policy Advisory Council](#) to allow for development of appropriate updates to policies.
- D. Violations of these policies may result in appropriate administrative action, up to and including revocation of system privileges, employee termination, or student expulsion. Users who fail to complete the required annual acknowledgement may also be subject to system access suspension until compliance is achieved.

## V. RELATED INFORMATION

- A. [Information Technology Services](#)
- B. [ITS Help Desk](#)
- C. [Email and Electronic Communications Policy](#)
- D. [User Account \(NetID\) Management Policy](#)
- E. [Intellectual Property Policy](#)
- F. [MSU Denver Faculty Employment Handbook](#)
- G. [MSU Denver Student Code of Conduct](#)
- H. [Prohibition Discrimination, Harassment, Sexual Misconduct, Title IX Violations, and Retaliation Policy](#)
- I. [EDUCOM: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community](#)

## VI. POLICY HISTORY

- A. **Effective:** June 1, 2026
- B. **Revised:** 2026 revisions include edits for brevity and clarity, removal of links to outdated documents, and addition of the required annual acknowledgement of this policy; January 1, 2022.
- C. **Original Enactment Date:** July 1, 2017
- D. **Review:** This policy will be reviewed every three years or as deemed necessary by University leadership.



**President's**  
Policy Statement  
University Policy  
Library

Operational Area	Information and Technology
Responsible Executive	Chief Information Officer
Responsible Office	Information Technology Services
Effective	June 1, 2026

## Acceptable Use of Computing Systems Policy

### Information and Technology

---

#### VII. POLICY APPROVAL

A handwritten signature in blue ink, appearing to read "Janine Davidson", written over a horizontal line.

Janine Davidson, Ph.D.  
President, Metropolitan State University of Denver

N/A  
\_\_\_\_\_  
Chair, Board of Trustees, Metropolitan State University of Denver