MARICOPA COMMUNITY COLLEGES | GOVERNING BOARD POLICY

B.P. 10.1

# Acceptable Use

**Policy Number:** 10.1
**Section**: Section 10 – Information Technology and Data Governance Policies
**Adopted Date:** 01/27/2026
**Effective Date:** 01/27/2026

## Purpose

The Maricopa County Community College District (MCCCD) is committed to providing technology resources that enable innovation, support teaching and learning, foster collaboration, and protect the integrity of our educational and administrative systems. In alignment with our vision to pursue excellence in education for a better world, and our mission to ignite talent, transform lives, and enrich communities, this Acceptable Use Policy (AUP) establishes clear expectations for the responsible and ethical use of MCCCD's information technology (IT) resources. These expectations are rooted in our institutional values: student centricity, integrity, collaboration, community, innovation, and respect, and are intended to guide users in the secure and appropriate use of technology to support our academic and operational goals.

## Scope

This document applies to all users of MCCCD’s IT resources. This includes but is not limited to students, faculty, staff, contractors, vendors, consultants, volunteers, and guests who access or use technology resources owned, operated, or maintained by MCCCD, whether on-campus or remotely. By establishing a uniform standard of acceptable behavior, MCCCD ensures its digital infrastructure remains secure, operational, and aligned with our institutional mission.

## Definitions

- Acceptable Use: Refers to the responsible, lawful, and ethical behavior expected from all individuals who access MCCCD technology. Users must:
    - Engage in activities that support academic, research, administrative, or community service functions.
    - Protect the integrity and confidentiality of data, especially sensitive or regulated information.
    - Abide by all applicable federal and state laws, as well as MCCCD's policies, administrative regulations, and ITS directives.
    - Respect others and the digital community by avoiding behavior that is disruptive, harassing, discriminatory, or otherwise harmful.
    - Use resources efficiently and avoid wasteful or excessive consumption.
    - Refrain from personal profit-making or partisan political activity using MCCCD systems.

  Use of MCCCD technology resources must comply with all district-wide policies.

- MCCCD Technology Directives: MCCCD ITS Directives
  These directives outline the standards for responsible technology use, including data security, access management, and system integrity. They serve as an extension of the Acceptable Use guidelines and must be followed by all users of district systems.

---

## Policy Statement

A. Prohibited Activities

This section outlines activities that are expressly forbidden due to risk to institutional integrity, legal compliance, and user safety.

Prohibited activities include, but are not limited to, the following:

- Accessing, hacking, or circumventing system security.
- Downloading or disseminating malware, viruses, or other harmful software.
- Using MCCCD IT resources for personal business, political campaigning, or fundraising.
- Accessing or distributing illegal content.
- Accessing or distributing pornographic content, subject to academic freedom protections.

- Engaging in software piracy or copyright infringement.
- Sharing confidential data without authorization.

B. Policy Review & Updates

This section describes MCCCD's commitment to continuous improvement in policy and governance.

This AUP is reviewed annually to ensure alignment with evolving security threats, regulatory requirements, and institutional practices, and to maintain consistency with MCCCD governance standards. It is the responsibility of all users to stay informed of changes and reaffirm their understanding when updates occur.

C. Annual Requirements to Maintain Access

This section details the proactive compliance actions users must take to retain access privileges.

All MCCCD-employed users must:

- Complete annual cybersecurity awareness training within the first 30 days of employment and on a yearly basis thereafter. (Access may be revoked until training is completed.)
- Comply with all ITS governance and cybersecurity directives.
- Acknowledge their responsibility to report security incidents or policy violations to CS@domail.maricopa.edu.

Failure to meet these requirements may result in suspension of IT access until compliance is achieved.

---

## Responsibilities

| Role or Office | Responsibility |
|---|---|
| All Users of MCCCD's IT Resources | Stays informed of changes and reaffirm their understanding when updates occur |

| | |
|---|---|
| Information Technology Services | Monitors compliance |

## Cross Reference(s)

AR 4.3 Electronic Communications

AR 4.4 Technology Resource Standards

## Legal Reference(s)

A.R.S. § 89-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions

20 U.S.C. 1232g. Family education and privacy rights

Public Law 105 – 304 – Digital Millenium Copyright Act

## Policy History and References

**Frequency of Review**: Annually

| Review Date(s) | Responsible Division | Revised Date(s) |
|---|---|---|
| | Information Technology Services | |