Status Active PolicyStat ID 17947402

Origination	12/2022
Last Approved	09/2025
Effective	09/2025
Last Revised	12/2022
Next Review	09/2027

Owner	Robert Gibbs: Chief Information Security Officer
Area	6000 Technology
Policy Numbers	6015

6015 Acceptable Use of Technology

Overview

This policy's purpose is to protect the availability and stability of Cochise College's Information Technology (IT) resources and to ensure equitable access to these resources by clearly defining acceptable use of them.

1. Scope

All users of college IT resources are expected to be aware of and understand how to comply with this policy while using any college technology resource.

2. Roles and Responsibilities

Users of college IT resources are expected to comply with this policy and bring questions to the Office of Technology Services (OTS) whenever they have a question regarding this policy or college IT resources.

OTS will configure, deploy, maintain, and monitor IT resources so that their users have a reasonable opportunity to access them and utilize them in compliance with this policy. OTS will implement controls and procedures to protect college IT resources from potential damage as a result of unacceptable use of IT resources.

College faculty and staff are expected to be aware of this policy sufficient to ensure their academic expectations, guidance, and advice to students is consistent with the intent of this policy.

College supervisors are expected to enforce this policy within their scope of responsibilities and bring any questions or concerns regarding this policy to the attention of the OTS.

3. Requirements

Acceptable Use:

Authorized users may utilize college IT resources for legitimate instruction, learning, research, academic support and professional services related to the scope of their position, so long as such use complies with these and all other policies of the college as well as local, state, and federal laws and regulations. In regards to the use of IT resources, authorized users are expected to:

- use resources only for legitimate instruction, learning, research, academic support and professional services consistent with the mission of the college;
- protect their user ID, password, and system from unauthorized use;
- access only information that the user owns, that is publicly available, or to which the user has been given authorized access;
- be considerate in the use of shared resources (i.e. network bandwidth, printers, file storage, lab/library/public computing resources, etc.);
- demonstrate respect for principles of open expression;
- demonstrate respect for and consideration of all other individuals
- comply with copyright laws and other restrictions on intellectual property as they apply to computer software and other materials that the user may access.
- be careful to ensure that their use of college IT resources does not represent a significant potential for exploitation by malicious entities, for introduction of malicious or unauthorized software, or for denial of use or disruption in the availability or accessibility of any IT resource.

Personal Use

Employee incidental personal use is an accepted and appropriate benefit for authorized users of the college's technology environment. Incidental personal use is acceptable when the use:

- is brief and irregular in occurrence;
- does not interfere with job performance;
- does not interfere with the access of others to the IT resources of the college;
- does not incur unexpected costs for the college;
- is not used for personal monetary gain;
- is not otherwise in conflict with the college's mission or in violation of any college policy.

Employee supervisors may restrict employee personal use where protection of college assets or department productivity is deemed at risk.

Personal use by students is permitted as long as it adheres to college policies and does not present risk of interference with instructional processes and the college's mission. Faculty and staff may restrict personal use by students in these situations.

While incidental personal use is permitted, users are strongly encouraged to conduct personal activities during personal time and utilizing non-college IT resources or, for authorized users, utilizing the college

housing, library and public-wifi networks.

Expectation of Privacy

The OTS is charged with ensuring the availability, confidentiality, and integrity of college information and also with implementing appropriate controls to enforce policy related to the use of college technology resources. Accordingly, the OTS will maintain the necessary capabilities for monitoring and analyzing usage of college applications, networks, and systems. Such capabilities include, but is not limited to the examination of contents of emails sent by or to any user and websites visited by any user. The OTS will ensure appropriate confidentiality is maintained, however, individual privacy related to use of college technology resources should not be expected.

Unacceptable Use:

College IT resources are provided for use by authorized users in accordance with this policy. Users are required to conduct their activities within the constraints of college policies and state and federal laws and regulations. Unacceptable use of college IT resources includes, but is not limited to:

- damage of computing facilities, programs, or data;
- access to, or copying of, college data or programs without proper authorization;
- allowing the reproduction of copyrighted material in any form without proper authorization;
- use of college IT resources that are not authorized to the user's account;
- sharing access codes, passwords, or individual user account access with other individuals;
- rendering any college IT resource inaccessible, inoperable, or significantly degraded;
- use of any college IT resource to abuse, defame, harass or threaten another individual or group, commit fraud or distribute other unlawful messages;
- use of any college IT resources for personal political or lobbying purposes;
- use of any college IT resource to create, display, share, or publish threatening, obscene, racist, sexist, or harassing material;
- use of college messaging systems (i.e. email, voice telephony, unified communications such as Zoom) outside of the mission of the college;
- directly connecting any unauthorized device to the networks in college's staff and faculty offices and data centers. Unauthorized devices are any devices not explicitly identified and approved by OTS for use within staff and faculty offices and data centers.
- storing of unauthorized data or installation of unauthorized software on any network or system in college staff and faculty offices and data centers. Unauthorized data is any data not directly related to the college's mission or business operations. Unauthorized software is any software that is not approved by the college OTS for use on the system on which it is installed.
- any other uses of college IT resources which are not in the best interest or part of the normal business of college.

4. Compliance

All use of college IT resources must comply with federal, state, and local laws and regulations to include

but not limited to the United States Copyright Law of 1976 and the Family Educational Rights and Privacy Act (FERPA).

5. Exceptions

Exceptions to this policy must be approved in writing by the college president.

6. Violations

The college, under the authorization of the Chief Information Officer, or designee has the authority to disable access to college IT resources of those found to be in violation of this policy.

The college shall enforce disciplinary action against users who willfully misuse or otherwise cause, through their use, damage to or reasonable potential for damage to college IT resources. Such actions may include, but are not limited to, limiting the accesses associated with the user's account, canceling the user's account, revoking access to resources, assessing discipline in accordance with applicable college policies, including discipline and potential termination of employment, and/or seeking prosecution under the laws of the State of Arizona where applicable.

Approval Signatures

Step Description	Approver	Date
Final Approval	Crystal Wheeler: Executive AdminiAssist President/ Governing Board	09/2025
Employee Senate (or assigned committee)	Wendy Davis: VP for Administration	04/2025
ADCAB	Wendy Davis: VP for Administration	04/2025
	Robert Gibbs: Chief Information Security Officer	04/2025