


# PROCEDURE MANUAL

		<b>PROCEDURE 223.001</b>	
		Page 1 of 4	
		<b>Last Revision Date:</b>	04-01-2024; 04-20-2023; 03-07-2022; 08-02-2021; 09-20-2020
		<b>Effective Date:</b>	09-20-2020
		<b>Last Review Date:</b>	04-01-2024
<b>Section:</b>	Technology	<b>Subject:</b>	Acceptable Use of Technology

## PURPOSE

The purpose is to outline the procedure Arizona Western College’s (AWC) Information Technology Services & Support (ITSS) takes to establish administrative guidelines to govern the use of the College's information technology resources consistent with the mission of the College.

## SCOPE

This procedure applies to all users of AWC information assets including employees, students, volunteers, and contractors.

## PROCEDURE

### 1. Access

1.1 Access to the College’s computer and network systems is limited to current AWC employees, students, volunteers, and contractors., who access these resources for legitimate research, teaching, learning, academic support and professional service, and whose use complies with these and other policies of the College. Students, faculty, staff, and guests are responsible for all use of their accounts and/or equipment.

### 2. Restrictions

#### 2.1 Federal Copyright Law

i Students, faculty, staff, and approved guests using the College’s computer and network systems are subject to the United States Copyright Law.

1 This legislation requires that users adhere to the restrictions that apply to the reproduction of software, as well as limit their copying to the boundaries permissible under the “fair use” doctrine.

#### 2.2 Local, State and Federal Laws

i All publications or broadcasts disseminated by the College shall conform to applicable regulations of the Federal Communications Commission and other applicable local, state, and federal laws.

- ii Students, faculty, staff, and approved guests are legally responsible for their communications.
- iii College facilities or properties may not be used for personal profit or for the profit of any private enterprise not for the benefit of the College.

### 2.3 Licensing Regulations

- i Arizona Western College has an established independent licensing program to regulate and restrict the use of the name, abbreviations, symbols, emblems, logos, mascots, slogans, and other terminology associated with the College.

## 3. Misuse of Privileges

3.1 The State of Arizona, local taxpayers and the U.S. Government provide Arizona Western College with computing and network resources.

3.2 Misuse of these finite and critical resources threatens their continued availability. Justification for the support of this system suffers when misuse occurs.

3.3 Students, faculty, staff, and approved guests who misuse computer or network privileges are subject to the loss of computer resources and/or network access and may also be subject to discipline and/or termination through college processes, as well as criminal or civil prosecution under federal and Arizona law.

3.4 Misuse of computing resources includes, but is not limited to, the following:

- i Using technology resources in a manner that violates the laws of the United States of America and/or the State of Arizona or that violates the policies of Arizona Western College.
- ii Unauthorized access to the resources of the College's computer systems or network (e.g., trying to log or break into accounts or computers for which you are not authorized).
- iii Disruption or obstruction of authorized use of the network.
- iv Failure to comply with all Computer Information Services Policies and Guidelines.
- v Knowingly causing excessive and unnecessary use of college resources such as staff time, network bandwidth, or computer capacity.
- vi Destroying the integrity of computer-based information or systems.
- vii Unauthorized use, or attempted unauthorized use, of the College's computer systems, computer networks, computer software, data files, or other computing facilities.
- viii Compromising the privacy of users, including misrepresenting or forging identities on, or using the College's network.
- ix Using College computer and networking systems for personal gain or commercial purposes unrelated to activities that support, and are consistent with, the educational purpose and mission of the College.
- x Using College computer networking systems and resources for obscene purposes or in a pervasively profane manner, including but not limited to use which may bring into public disrepute the College's identity and image.
- xi Theft, distribution, or reproduction without lawful authority of copies or reproductions of property or subject matter of any kind belonging to another,

including but not limited to that which is protected by federal, state, or international law governing patent, copyright, trademark, trade name, trade secrets, privacy, publicity, unfair competition, or licensing agreements.

xii Tampering with computer software or data files belonging to others or using the resources in such a manner that would cause the College to believe that it would be subject to the risk of suit or regulatory action.

xiii Using resources in a manner that is likely, or with the intention, to inflict mental harassment, to intimidate, or unreasonably to invade the privacy of any other individual.

xiv Knowingly accessing, downloading, displaying, or transmitting sexually explicit images or language, including accessing web sites that display such images or language, unless such action is taken in furtherance of legitimate research or educational purposes.

xv Accessing, downloading, displaying, or transmitting material intended to provide information or instruction regarding how to access information the user is not authorized to access or how to disrupt the functioning of any computer system or network (i.e., “hacker websites”), unless such action is taken in furtherance of legitimate research or educational purposes.

xvi Sharing College account passwords with others or using networked machines to provide College network access to people or organizations that do not already have such access.

xvii Using technology resources to post material on behalf of other parties, sharing personal access to the College’s resources with others, or using personal computers connected to the College’s network to mirror another site (i.e., to make a copy of someone else’s site).

xviii Unauthorized installation of software on the College’s computers, networks, or network devices.

xix Using technology resources to threaten any individual with violence or to engage in any activity that would naturally and directly tend to provoke acts of violence or a breach of the peace by the person to whom the conduct or remarks are addressed.

xx Using technology resources in a manner that would lead the College reasonably to believe that such use may subject it to the risk of suit, regulatory action, or liability of any kind under the laws of the United States of America or the State of Arizona forbidding the creation or maintenance of a hostile working or educational environment involving discrimination based on race, color, sex, religion, national origin, age, veterans’ status or disability, whether physical or mental, or which would cause the College reasonably to believe that such use of its property and resources may result in a determination that it is in breach of its legal duty to take reasonable steps to eliminate such attributes, conditions, or vestiges of a hostile educational environment and/or of discrimination.

#### 4. Institutional Discipline

##### 4.1 Any individual or group that:

- i Uses technology to participate in conduct that is in violation of this policy,
- ii Uses technology to adversely affect the College's pursuit of its educational objectives,
- iii Uses technology to violate or show disregard for the rights of individuals within the College community, or
- iv Uses technology to damage property
- v May be subject to institutional discipline. Officials charged with enforcement of these regulations shall have the authority in execution of such duties to immediately perform such acts as are required to maintain the security, well-being, and safety of college resources, the College community or any of its members.

5. Expectation of Privacy

5.1 The College's administrators reserve the right to suspend or examine any account, computer, or network access information, including the content of emails sent by or to any network user and the websites visited by any user.

5.2 Users of this system do not have an expectation of privacy in their use of the College's network or computer system. Any instance of misconduct will be reported to the appropriate College office.

6. Hold Harmless Agreement

6.1 The account holder agrees to be responsible for, and to indemnify and hold the Arizona Western College District Governing Board, Arizona Western College, and their officers and employees harmless from any claims, including attorney's fees, resulting from the account holder's acts or omissions which cause direct or indirect damage to another party.