ACCREDITATION EVIDENCE

Title: Policy 2180A: Acceptable Use of Computing Resources

Evidence Type: Clear

Date: 23 June 2022

WAN: 22-0425

Classification: Policy

PII: No **Redacted:** No

ACCEPTABLE USE OF COMPUTING RESOURCES

References: Family Educational Rights and Privacy Act, 20 U.S.C. §1232g; 34 CFR 668.14(b)(30); Higher Education Opportunity Act of 2008 (HEOA) (Pub. L. 110-315); Section 504 of the Rehabilitation Act of 1973; ED Section 508; Title II of the Americans with Disabilities Act of 1990; Board Policy 3910I

The computing resources at Western Wyoming Community College (the College) are available to support the educational, instructional, research, community, and administrative activities of the College. The use of these resources is a privilege that is extended to members of the College community. As a user of these services and facilities, the user has access to valuable College resources, sensitive data, and internal and external networks. Consequently, it is important for that individual to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, maintaining the integrity of the physical equipment, adhering to all cybersecurity requirements, and following all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the College will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the College. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change. Violation of said laws may result in prosecution to the full extent of the law.

This policy applies to all users of computing resources owned or managed by the College. Individuals covered by the policy include College faculty and visiting faculty, staff, students, alumni, guests or agents of the administration, external individuals, and organizations accessing network services via the College's computing facilities.

Computing resources include all College owned, licensed, or managed hardware and software, and use of the College network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by the Information Technology Services department, personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the College's network services.

User Responsibilities

The College shall provide the use of scholarly and/or work-related tools, including access to computer labs, certain computer systems, servers, software and databases, the campus

telephone and electronic communication systems, and to the Internet. The user has a reasonable expectation of unobstructed use of these tools, certain degrees of privacy (which may vary depending on whether the individual is an employee of the College or a matriculated student, see the Privacy Policy for more information), and protection from abuse and intrusion by others sharing these resources. The user can expect the privilege of accessing information and expressing an opinion that is as protected as if it is for paper and other forms of non-electronic communication.

In turn, the user is responsible for knowing the regulations and policies of the College that apply to appropriate use of the College's technologies and resources. The user is responsible for exercising good judgment in the use of the College's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action. See the Information Technology Services Handbook for a detailed listing of all IT-related procedures.

Acceptable Use

- Users may utilize only the computers, computer accounts, and computer files for which authorization has been granted. The user may not attempt to obtain system privileges not previously authorized.

- Users may not utilize another individual's account, or attempt to capture or guess other users' passwords. No one will give any password or user ID for any of the College's technology resources to any unauthorized person.

- Users are responsible for appropriate use of all resources assigned to that individual, including the computer, phone, the network address or port, software, and hardware. Therefore, the user is accountable to the College for all use of such resources. As an authorized College user of resources, the user may not enable unauthorized users to access the network by using a College computer, user account, or a personal computer that is connected to the College network.

- The College is bound by its contractual and license agreements respecting certain third-party resources; the user is expected to comply with all such agreements when using such resources.

- Any user who determines that someone has made an unauthorized use of his or her account, password or user ID, will report that breach of security to the College's Chief Information Officer and Information Technology Services department.

- The user should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. The user must configure hardware and software in a way that reasonably prevents unauthorized users from accessing the College's network and computing resources.

- The user must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

- The user must comply with the policies and guidelines for any specific set of resources to which the user has been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

- The user must not use College computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

- On the College network and/or computing system, the user is not authorized to use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless specific authorization has been granted by the Chief Information Officer.

- The user shall not use the College's technology resources for illegal, commercial or profit-making purposes.

- The user shall not use the College's technology resources to engage in any form of academic dishonesty, such as plagiarism or cheating.

- The user shall not attempt to endanger or breach the security or operation of any of the College's technology resources.

- The user shall not run nor distribute a program on any of the College's technology resources, unless the user is confident that the program will not harm or endanger the system.

- The user shall not knowingly create, install or distribute a computer virus or any other type of destructive program on any of the College's technology resources or otherwise damage or destroy any equipment, software or data belonging to the College or any other user.

- The user shall not, without proper authorization, modify or reconfigure the software or hardware of any of the College's technology resources.

- The user shall not use any of the College's technology resources in a manner that violates the privacy of other users.

- The user shall not, without proper authorization, access, read, copy, alter or delete any other person's computer, files, electronic mail, or account information.

- The user shall not create, install, or distribute any program that is designed to trick or deceive user into revealing confidential information about themselves.

- The user shall not use any of the College's technology resources to access or transmit images, messages, communications or other materials that can be deemed to be obscene, threatening, harassing, annoying, defamatory, fraudulent, or unlawful.

- The user shall not misrepresent his or her identity or relationship to the College when obtaining computing or network privileges, or when using any of the College's technology resources or in any electronic communication with anyone else.

- The user shall not falsely attribute or forge the origin of electronic mail, messages or postings.

- The user shall not install, copy or otherwise use any software or data in violation of applicable copyrights or license agreements. The user will not make nor distribute unauthorized copies of software or data contained in the College's technology resources, nor will anyone install or use unauthorized or pirated software on any of the College's technology resources.

- The user shall only communicate or distribute electronic mail to clearly identified groups of interested individuals who may reasonably be expected to want to receive the transmission, and will not engage in the mass broadcasting of electronic mail nor the distribution of chain letters.

- The user shall not send electronic mail to unwilling recipients, nor participate in the distribution of unsolicited commercial advertising ("spam") through electronic mass mailings. The user will comply with the 2009 CAN-SPAM Act.

- The user shall not post any documents or pages on the College's websites that do not comply with these rules, the Web Governance policy, or the Publications Manual.

Fair Share of Resources

Information Technology Services, and other College departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The campus network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use

them. Therefore, the use of any automated processes to gain technical advantage over others in the College community is explicitly forbidden.

The College may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

Adherence with Federal, State, and Local Laws

The user is expected to uphold local ordinances and state and federal law. Some College guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of the College's computing and network resources the user shall:

- Abide by all federal, state, and local laws.
- Abide by all applicable copyright laws and licenses. The College has entered into legal agreements or contracts for many of its software and network resources which require each individual using them to comply with those agreements.
- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
- Not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless the user has a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and/or criminal prosecution.

Other Inappropriate Activities

Other prohibited activities include:

- Activities that would jeopardize the College's tax-exempt status
- Use of the College's computing services and facilities for political purposes
- Use of the College's computing services and facilities for personal economic gain

Privacy and Personal Rights

While the College does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems for troubleshooting purposes, determining if an individual is in violation of this policy, or, as may be necessary, to ensure that the College is not subject to claims of institutional misconduct.

Access to files on College-owned equipment or information will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the Chief Information Officer in conjunction with requests and/or approvals from senior leadership positions of the College. External law enforcement agencies may request access to files through valid subpoenas and other legally binding requests. All such requests must be approved by the Chief Information Officer. Information obtained in this manner can be admissible in legal proceedings or in a College hearing.

In order to ensure the integrity of the College's technology resources and compliance with the rules set forth above, the College specifically reserves for itself the right to monitor, inspect and review any and all systems, files, data, mail, communications and other transmissions created, compiled, accessed, stored, or sent on any of the College's technology resources. Furthermore, in order to ensure the integrity of the College's technology resources, the College specifically reserves the right to immediately suspend, without any advance notice, the network and computing privileges of any user who is alleged to have misused or abused any of the College's technology resources. The College, in addition, reserves the right to discard incoming mass mailings that involve unsolicited commercial advertising ("spam") without notifying the sender or recipient, as well as the right to block all Internet communications from sites that are involved in extensive mass mailings or other disruptive practices or which contain sexually explicit content or other content that is, in the opinion of the College, inconsistent with its mission.

Privacy in Email

While every effort is made to insure the privacy of College email users, this may not always be possible. In addition, since employees are granted use of electronic information systems and network services to conduct College business, there may be instances when the College, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user.

User Compliance

When utilizing College computing services, the user accepts any College issued computing accounts, and must agree to comply with this and all other computing related policies. The user has the responsibility to keep up-to-date on changes in the computing environment, as published, using College electronic and print publication mechanisms, and to adapt to those changes as necessary. All proceedings are published in the Information Technology Services Handbook.

The rules set forth above are intended to help authorized users use the College's technology resources responsibly and in compliance with the applicable laws. The rules are not intended to be exhaustive, and the College specifically reserves the right to add to and modify these rules within its discretion. The College also specifically reserves the right to enforce its interpretation of these rules, as well as the right to discipline a user or limit, suspend or revoke a user's ability to use the College's technology resources if the College, in its opinion, believes that the user has misused or abused those resources, even though the user's particular conduct may not be specifically listed in the rules above. All users of the College's technology resources are responsible for being aware of and complying with this policy, as well as with all of the College's other pertinent policies and procedures.

The College seeks to provide users with a stable and reliable computer network, the College cannot guarantee against a loss of data, files and/or software as a result of system crashes, network outages, power outages or similar interruptions in service. Accordingly, the College disclaims any liability for loss of data, damages, service interruptions or failure to deliver services. The College also disclaims any responsibility and/or guarantees for data, information and materials contained in systems or sites not developed by the College, such as those obtained through the Internet.

If a user suspects any violation of the above rules, the user should notify the College's Chief Information Officer. Users of the College's technology resources are expected to cooperate with the Chief Information Officer in the operation of these resources and the investigation of any misuse or abuse.

Proposed November 18, 2021