Board Procedure 500.7: Acceptable Use of Technology & Computing Resources
Students

Purpose
This procedure establishes expectations for acceptable use of Iowa Valley Community College District (IVCCD) technology resources by students, in support of teaching, learning, and college operations. IVCCD technology resources are provided to enable academic success, facilitate communication, and conduct official college business.

Scope
This procedure applies to all students and to all IVCCD technology resources they use or access, whether on campus or remotely. Technology resources include, but are not limited to, computers, mobile devices, networks and wireless access, learning management systems, email, cloud services, software and applications, printers, and any other systems or services owned, licensed, or managed by IVCCD.

Guiding Principles
Access to IVCCD technology resources is a privilege, not a right, and may be limited, suspended, or revoked when misused.

Students are expected to use technology resources in ways that are ethical, respectful, academically honest, and compliant with law and college policies.

Use of IVCCD technology resources should prioritize educational and college-related activities. Reasonable personal use, including streaming, gaming, and other online services in housing and common areas, is permitted when it does not interfere with academic or business use, degrade network performance for others, or violate any policy or law.

Students are responsible for all computing operations executed under their accounts and usernames.

Privacy and Monitoring

IVCCD strives to balance academic freedom and privacy with its obligations to protect institutional resources, comply with law, and maintain a safe learning environment. The District may monitor, log, access, and review activity on its systems and networks, including email and stored data, without additional notice where authorized by law or policy, for operational, security, or compliance purposes. Students should not expect privacy in information created, transmitted, or stored using IVCCD technology resources, and such records may be subject to public records requests, litigation holds, audits, or other disclosures as required by law. The District reserves the right to keep logs of user activity for accounting, resource allocation, system and network usage analysis, and to use information gained in disciplinary or criminal proceedings, as permitted by federal and state law.

Acceptable Use Expectations

Students using IVCCD technology resources are expected to:

Use technology primarily for course work and college activities

Use technology resources for course work, research, communication with college personnel, and other college-related activities. Reasonable personal use (such as streaming, gaming, and social media) is allowed, particularly in student housing, so long as it does not interfere with the performance, security, or availability of IVCCD technology resources for academic and operational purposes or violate this procedure or other college policies.

Protect credentials and accounts

Use strong passwords, secure devices, and never share login information with anyone else. Students are solely responsible for all activity under their usernames and passwords. Sharing a username and/or password is prohibited. Disguising an identity to acquire a username falsely is prohibited.

Use only authorized resources

Use only accounts, devices, and services for which authorization has been granted, and only for purposes for which access is intended. Do not transfer or confer computing privileges to other individuals (except for authorized IT administrators).

Respect others

Communicate in a professional and civil manner, and avoid harassment, threats, or other abusive behavior when using college technology resources. All users are entitled to use IVCCD technology without being subjected to discriminatory behavior based on

race, color, ancestry, religion, national origin, disability, age, gender, or sexual orientation.

Respect intellectual property
Comply with copyright, software license agreements, and intellectual property rights when accessing, using, or sharing digital content and applications. The District recognizes and adheres to U.S. and International copyright laws, software licenses, and intellectual property rights. Software use must conform to copyright laws and licensing agreements.

Protect sensitive information
Follow District guidance on storage, sharing, and transmission of confidential and sensitive information, including student education records (FERPA).

Report security concerns
All users have the responsibility to report to the District's IT department any observed or known copyright infringement, security incidents, suspected account compromise, or unusual system behavior.

Unacceptable Use
The following activities are examples of prohibited student use of IVCCD technology resources; this list is illustrative and not exhaustive.

Illegal or unethical activities

- Violating federal, state, or local law (for example, harassment, stalking, threats, discrimination, identity theft, or child exploitation).
- Infringing copyright or other intellectual property rights, including unauthorized peer-to-peer file sharing of music, videos, or software, or unauthorized copying, installation, downloading, distribution, or duplication of software (including operating systems, programs, applications, databases or code) that is licensed or protected by copyright.
- Posting credit card numbers or passwords in publicly accessible locations on computer systems.

Security violations and system abuse

- Attempting to bypass or defeat security controls, circumvent normal resource limits, logon procedures, or security regulations, gain unauthorized access ("hacking"), or test vulnerabilities without written authorization.
- Introducing or distributing malware, viruses, worms, Trojans, or other rogue programs, or intentionally disrupting, degrading, or attempting to crash system performance or network availability.
- Connecting or installing unauthorized devices or equipment that alter or extend the IVCCD network or systems (such as personal routers, wireless access points, network sniffers, port scanners, network-attached storage, or servers).
- Attempting to modify or remove computer equipment or other equipment supporting information technology, software, or peripherals without proper authorization, including unauthorized alteration of system configuration, BIOS settings, and operating system settings.

Misuse of accounts, identities, or resources

- Sharing passwords or allowing others to use one's IVCCD account, or using another person's account, identity, or login credentials.
- Taking advantage of another user's naiveté or negligence to gain access to any account, data, software, or file without explicit authorization.
- Masquerading as another individual or entity, or sending deceptive, fraudulent, or anonymous communications intended to mislead or harm.
- “Spamming,” “mail bombing,” resource-hogging (such as excessive online gaming, high-volume media streaming, or excessive storage of personal documents, pictures, or media files on network servers), or otherwise consuming excessive resources in ways that interfere with others’ use or employee productivity.
- Using IVCCD technology resources for commercial purposes, personal financial gain, or operating personal business ventures.

Inappropriate content and conduct

- Accessing, creating, viewing, storing, copying, generating, transmitting, or distributing material that is obscene, sexually explicit, profane, or otherwise inconsistent with a professional and educational environment, except where explicitly authorized for legitimate academic purposes. This includes the intentional viewing, display, or printing of inappropriate materials.
- Using technology resources to harass, bully, intimidate, threaten, or abuse others, including through social media, messaging platforms, or collaboration tools. Any messages with derogatory or inflammatory remarks about any individual or group's race, color, ancestry, religion, national origin, physical or mental attribute, age, gender, and/or sexual orientation are prohibited.
- Displaying or transmitting content that is defamatory, libelous, or that incites violence or unlawful activity.
- Physically interfering with other users' access to the District's computing facilities.

Misuse of college information and identity

- Representing personal opinions as official positions of IVCCD or misusing college logos, names, or trademarks.
- Altering, destroying, or stealing data, records, or equipment, including attempts to interfere with logging, monitoring, or security controls.
- Disclosing or removing proprietary information, software, or other stored data (in any physical or electronic format) without explicit permission.
- Accessing, viewing, or attempting to access another user's data, files, email, voicemail, or other electronic information, whether on screen, in printed form, or through electronic means, without explicit permission.

Email and Collaboration Tools
IVCCD provides student email and collaboration tools (e.g., learning management systems, messaging, videoconferencing) as official channels for academic and District communications. Students are expected to:

- Check their District email and official communication platforms regularly and respond in a timely manner where appropriate.
- Use professional, respectful language and avoid content they would not be comfortable being retained, forwarded, or disclosed.
- Avoid transmitting confidential or sensitive information outside secure District systems unless authorized and appropriate safeguards are in place.
- Refrain from using District email and collaboration tools for commercial purposes, personal business ventures, mass solicitations, chain letters, or solicitations for business schemes.
- Protect access to email accounts and not share passwords.

Personally Owned Devices (Bring Your Own Device)
Students may use personally owned devices (laptops, tablets, smartphones, etc.) to access IVCCD resources, subject to this procedure and other applicable policies. When doing so, students must:

- Ensure their devices are secured with up-to-date operating systems, security patches, and antivirus or endpoint protection where applicable.
- Use secure network connections and avoid circumventing IVCCD security controls or content filters.
- Connect only to authorized IVCCD networks (such as the guest wireless network) and not attempt to access networks or systems for which they lack authorization.
- Understand that limited technical support may be available for personally owned devices and that access to District systems may be disabled if a device is compromised or poses a risk to the network.

Data Security and Incident Reporting
Students share responsibility for protecting the confidentiality, integrity, and availability of IVCCD information resources. Students must:

- Immediately report suspected security incidents, such as lost or stolen District devices, suspected account compromise, theft or unauthorized disclosure of confidential information, or unusual system behavior, to the IVCCD IT department.
- Follow any additional data protection requirements communicated for specific programs, systems, or clinical/field-based placements.

Ownership and Disclaimer
Technology resources and accounts provided by the District are owned by the District and are intended primarily for college-related activities. Information and data created, stored, or transmitted on District technology resources may be treated as District property, subject to applicable law and policy. The District does not guarantee that technology services will be uninterrupted or error-free and is not liable for loss of data or damage to data or services arising from use of its technology resources.

Enforcement and Consequences
Violations of this procedure may result in disciplinary or administrative actions, which can include, but are not limited to, a warning, required education, temporary or permanent suspension or revocation of technology access privileges, and referral to the student conduct process. Serious or repeated violations may also result in academic sanctions, removal from programs, disciplinary action up to and including suspension or expulsion from the District, and/or referral to law enforcement or external agencies where applicable, including possible legal and civil actions.

Any student's technology privileges may be suspended immediately upon the discovery of a possible violation of this procedure. Such suspected violations will be confidentially reported to the appropriate District official(s) and investigated in accordance with the procedures outlined in the student handbook and related policies. Procedures for investigation, notice, and appeal will follow the student conduct and disciplinary processes described in the student handbook and related policies.

The District reserves the right to extend, limit, restrict, or deny access to computing resources and to disable a user's access to technology resources at any time.

Date of Review: February 11, 2026
Date of Revision: February 11, 2026
Date of Adoption: June 11, 2014

Legal Reference
Iowa Code Chapter 22; Family Educational Rights and Privacy Act (FERPA)

Related Administrative Rules and Regulations
Board Policy 407; Student Code of Conduct

Revision History
May 10, 2023; December 12, 2018; October 10, 2018

Formerly Board Policy 524