



Board Procedure 400.8: Responsible Use of Computing Resources

Personnel

Privacy and Confidentiality

Iowa Valley Community College District's computers, networks, internet, email, and other information technology resources are only for academic and college-related business purposes. With limited exceptions, information, communications, and data stored in the District's information systems are considered public records under the Iowa Open Records Law, Iowa Code Chapter 22. Employees do not have a reasonable expectation of privacy when using the District's computers, networks, internet, email, and other information technology resources. The District reserves the right to log, access, or otherwise monitor any information stored on or passing through its systems or facilities for any reason without notice or consent. Information resulting from or residing on District systems may be subject to disclosure under the Iowa Open Records Law, in litigation, or for audit purposes.

Internet

The internet is a valuable resource for advancing the District's mission; however information or materials may be controversial, offensive, or inaccurate. Any and all access to and use of information or materials obtained via the internet is at the user's own risk. The District will rely on each individual to act responsibly and appropriately in the use of District information resources.

It is expected that each employee will abide by the law and District policies when accessing the internet.

Individuals will be responsible for and may be held liable for any unacceptable use of the internet. The District assumes no responsibility or liability for any wrongful use by individual employees.

Email

Electronic mail (email) accounts will be provided to all employees. Appropriate use of email is expected. Keep email free of personal opinions and inappropriate commentary. Never create a message that you would not want to become public.

Do not use email to communicate confidential or personal information outside of the District without proper security safeguards. Do not send anonymous, deceptive, fraudulent, or other unwelcome communications such as chain letters or solicitations for business schemes. The District's email system should not be used for personal gain. Protect access to your email account. Do not share your password.

Email Retention

This email retention guideline is in accordance with the District's Records Retention Policy 750. For retention purposes there are four categories of message value:

- Records Retention Policy 750 Related – Primary or supporting emails for records indicated in Records Retention Policy 750 should be stored accordingly, which includes:
 - Saving the email to the District's content management system
 - Saving as a PDF and storing on the appropriate file server
 - Printing the email and filing it in the appropriate location
- Transitory Value – Many emails are created primarily for informal communication and do not have lasting value. These emails should be retained until read, and then deleted.
- Temporary Value – Emails in this category have temporary “working” value and may be retained in your mailbox up to two years and deleted when no longer of value.
- Lasting Value – when contents contain information that has longer term value they may be classified as “Lasting Value” Examples include:
 - Document important actions taken or planned
 - Have legal or evidential value
 - Have historical significance
 - Document important information that may need to be referenced in future

These emails should be moved to the employee's "archive folder." There is no single retention period for these messages. The value of the email is based upon its informational content and should be retained and deleted accordingly. Emails left in employees' inboxes for more than two years and not moved to the archive folder will be automatically removed by the system. Please contact your supervisor if classification assistance is needed.

When litigation against the District or its employees is filed or threatened, the law imposes a duty upon the District to preserve all documents and records that pertain to the litigation. A litigation hold overrides the District's email retention policy.

Web

The World Wide Web (WWW or Web) allows the District to have a presence online and to provide information and educational services. The District's official websites represent the programs, policies, and overall image. Modifications to the District's websites should only be made by those authorized to do so.

The development of unofficial web sites by the District's departments, staff, and students (as part of an instructional activity) is permissible, but the District will not be held liable for the content of personal web sites. Individuals will act responsibly and appropriately when developing personal web sites.

Responsible Use

The user is responsible for the material that they choose to access, send, or display. Respect the privileges of others by complying with all District policies and guidelines. Remember that you are representing the District in all of your communications.

Use only login IDs and information technology resources for which you are authorized, and use them for the purposes for which they were intended. Do not let others use your login ID and password.

Unacceptable Use

Unacceptable use of computing resources may result in suspension or revocation of computer privileges and may include disciplinary action as well as possible legal and civil action, such as an infringement action by the copyright owner or disciplinary action by the District. Examples of unacceptable computer use include, but are not limited to:

- Unauthorized copying of any software (including operating systems, programs, applications, databases, or code) that is licensed or protected by copyright.
- "Computer hacking" (i.e. unwanted or unsolicited entry into a computer system).
- Knowingly introducing a "computer virus" or other unauthorized programs (either harmless or damaging) to the District's computers or network.
- Unauthorized access, willful damage, or misuse of systems, applications, databases, codes, or data.
- Use of the District's network, the internet, or other information technology resources for actions that constitute abuse, harassment, libel, slander, fraud, misrepresentation, or intimidation. This includes the introduction of inappropriate materials to the network, the intentional viewing or display of inappropriate materials, and the printing of inappropriate materials.
- Using the District's computing resources to conduct personal business for one's own personal benefit or profit, for the personal benefit or profit of others, for solicitation of services, or for political lobbying or campaigning.
- Allowing others to use your login ID and password to access the District's systems or using another person's login ID and password to access the District's systems.
- Use of District logos without prior approval.

Personal Use of District Information Technology Resources

District computers, equipment, and resources are to be used to support its teaching, training, research, service, and administrative functions. Occasional, limited personal use is permitted under conditions:

- Any use is brief.
- Any use occurs infrequently.
- The use does not interfere with the performance of the employee's duties.

- The use does not compromise the security, performance, or integrity of District property, networks, information, or systems.

Observation of of Unacceptable Use

Any individual observing or learning of unacceptable use should report the violation to the appropriate District personnel (i.e. student to instructor/staff; staff to supervisor; faculty to dean; or to the Vice President of Administration). Personnel who receive the initial report of unacceptable use may, depending on severity, report the violation in writing to the appropriate Executive Leadership Team (ELT) member. The ELT member should notify the President. All disciplinary action will be in accordance with Board Policy 421 - Disciplinary Action. If the violation could be a violation of state or federal laws, the ELT member must communicate the violation to the President.

User Violation: Consequences, Notifications, and Appeal

A violation of Board Policy relating to responsible use of computing resources will be referred to the employee's supervisor for appropriate disciplinary action. The sanctions to be imposed will be determined on a case-by-case basis and may vary from a written warning to termination of employment, depending upon the severity of the offense and the number of prior violations, among other things. Employees adversely affected by such disciplinary action may resort to the appropriate grievance procedure.

Date of Review: July 16, 2025

Date of Revision: July 16, 2025

Date of Adoption: June 11, 2014

Legal Reference

Iowa Code Chapter 22

Related Administrative Rules and Regulations

Board Policy 412

Revision History

May 10, 2023; October 10, 2018

Formerly Board Procedure 407.1; Board Policy 407