Instruction

Administrative Procedure – Acceptable Use Procedure (AUP):

AUTHORIZATION FOR ELECTRONIC NETWORK ACCESS AND COMPUTER USAGE

'Electronic Network(s)' or 'Network(s)' is defined as the District's network (including the wireless network), servers, computer workstations, mobile technologies, peripherals, applications, databases, online resources, Internet access, email, digital accounts, and any other technology designated for use by students and staff, including all new technologies as they become available. If a user accesses the District's electronic networks, including Internet service or Wi-Fi, with a personal technology device, that use is also considered use of "electronic networks" that is covered by this Agreement

All use of Electronic Networks, including the Internet, must (1) be for the purpose of educational research; (2) be consistent with the educational objectives and curriculum adopted by the District, as well the varied instructional needs, learning styles, and abilities of the students and (3) comply with all the Exhibits presented in Section 2 of this Administrative Procedure 6:235: AP1.

The failure of any user to follow the terms of the *Authorization for Electronic Network Access and Computer Usage* and all associated Exhibits will result in the loss of privileges, disciplinary action, and/or appropriate legal action. Agreeing to these terms during the registration process for students or the hiring process for adults indicates that you have carefully read and fully understand these

Section 1: Terms and Conditions

Acceptable Use

Access to the District's network and Internet must be for educational or research purposes and must be consistent with the District's educational objectives.

1. Privileges – The use of the District's network and Internet is a privilege, not a right, and inappropriate use will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The Superintendent (or their designee) will make all decisions regarding whether a user has violated these rules and will make the appropriate recommendations.

2. Students and staff should have no expectations of privacy regarding use of the network. Network administrators, including system administrators, have access to all information associated with electronic communication.

Unacceptable Use

Any student or adult issued a District network account is responsible at all times for using it properly, as outlined in this procedure. The following are examples of unacceptable use and are not meant to be an exhaustive list:

1. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation.
    a. Streaming media providers such as Netflix, Hulu, and Amazon explicitly deny the use of their products outside of home use. The following are examples of third-party policies restricting public viewing:
        i. Amazon: http://bit.ly/2mad7U1; refer to 4h ii.
        ii. Hulu: https://hulu.tv/2mcVF1i; refer to 3.2 iii.
        iii. Netflix: http://bit.ly/2m4W7hU
2. Unauthorized uploading or downloading of software, regardless of whether it is copyrighted or unlicensed.

3. Using the computer system for private financial or commercial gain (this includes buying or selling on the Web).
4. Wastefully using resources, such as file space, personal multimedia, chain letters, flaming, etc.
5. Gaining unauthorized access to resources or entities.
6. Trespassing in others' folders, work, files, or changing computer files not belonging to the user;
7. Invading the privacy of individuals.
8. Using another user's account or password or sharing passwords with others.
9. Posting material authored or created by another without his/her consent.
10. Posting anonymous messages.
11. Using the network for commercial or private advertising.
12. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening (including weapons & bombs), racially offensive, harassing, or illegal messages, pictures, or other material.
    a. Using the network or Internet while access privileges are suspended or revoked.
    b. Using chat rooms and/or social networking sites without permission.

Network Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Being polite. Not becoming abusive in messages to others.
2. Using appropriate language. Not swearing, or using vulgarities or any other inappropriate language.
3. Not revealing ANY personal addresses or telephone numbers.
4. Recognizing that electronic mail (E-mail) is not private. Administrators of the system have access to all mail, files, and activity logs. Messages relating to or in support of illegal activities must be reported to the authorities.
5. Not using the network in any way that would disrupt its use by other users.

No Expectation of Privacy

Users of the District's electronic networks have no expectation of privacy with respect to use of the District's electronic networks, including access to the District's Internet or Wi-Fi using personal technology, or with respect to any material created, transmitted, accessed, or stored via District electronic networks. This includes material created, transmitted, accessed, or stored for personal use, including incidental personal use, on or through the District's electronic networks. The District reserves the right to monitor users' activities on District electronic networks at any time for any reason without prior notification; to access, review, copy, store, and/or delete any electronic information accessed or stored therein; and to disclose such information to others as it deems necessary and/or as required by law. Users should be aware that information may remain on the District's electronic networks even after it has been deleted by the user.

Use of Cloud Applications (Hosted and Non-Hosted)

The District provides staff and students with both Microsoft 365 and Google Workspace for Education accounts, including Word, Gmail, Docs, Classroom, and other tools. The District controls app access to ensure

educational use. For details on Microsoft's data practices, review their Privacy Statement. For details on Google's data practices, review their Privacy Notice. By agreeing, you consent to the use of Microsoft 365 and Google Workspace for Education, as well as their respective third-party services. Contact the district with any concerns before making a decision.

Use of Electronic Mail

The District's electronic mail system, along with its constituent software, hardware, and data files, is owned and controlled by the School District.

- The District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an educational tool.
- Electronic mail is not private. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Electronic mail messages containing illegal or other information in violation of this policy will be reported to the appropriate official immediately. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
- Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.
- Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the school district. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this school district. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- All e-mail messages must conform to the acceptable use policy for the District's electronic networks.

Instructional Resources and Digital Accounts

Users may be granted access to online instructional resources to create a collaborative online environment. The purpose of this access is to create an online environment where users can display and share their creations. Users will have the opportunity to create websites, multimedia posters, podcasts (audio recording), and videos utilizing educational resources, including but not limited to learning platforms, blogs, wikis, and podcasts. Users understand that their work may be viewed by others in a public digital format; therefore, users will not reveal personal information. Participation in these resources may require individual digital accounts. District staff will control student accounts.

Student Online Personal Protection Act (SOPPA)

Protecting student data is a priority for the Moline-Coal Valley School District and of the utmost importance. Our District leverages the **Student Data Privacy Consortium** (**SDPC**) to determine if educational technology companies are in full compliance with state and federal privacy laws. The following resources provide additional information about what happens to our students' data and the measures we take to protect their privacy. See 7:345-AP-E2 for the full procedure.

Website Accessibility

The District is committed to ensuring the accessibility of its website for students, parents, and community members with disabilities. All pages on the District's website will conform to the W3C Web Accessibility Initiative's (WAI) Web Content Accessibility Guidelines (WCAG) 2.0, Level AA conformance, or updated equivalents of these guidelines.

The District is committed to compliance with the provisions of the Americans with Disabilities Act (ADA), Section 504 and Title II so that students, parents and members of the public with disabilities are able access, engage and enjoy the same benefits and services within the same timeframe as those without disabilities, and are not excluded from participation in, denied the benefits of, or otherwise subjected to discrimination in any school district programs, services, and activities delivered online.

Please review the District's full Accessibility Statement for more information and to find procedures for filing a complaint for non-compliant District resources.

Bring Your Own Device (BYOD)

A personally owned device shall include all existing and emerging technology devices that can take photographs, record audio or video, input text, upload and download media, and transmit or receive messages or images. Examples of personally owned devices include, but are not limited to: streaming media players, iPads and other tablet PCs, laptop and netbook computers, cell phones and smartphones (such as iPhones), as well as any device with similar capabilities. All such devices must comply with the Authorization For Electronic Network Access And Computer Usage (6:235-AP1) and all associated exhibits.

1. Educational purposes include classroom activities, career development, communication with experts, homework, and limited high-quality self-discovery activities. Staff and students are expected to act responsibly and thoughtfully when using technology resources. Staff and students bear the responsibility to inquire with school administrators when they are unsure of the permissibility of a particular technology use before engaging in it.
2. District Administration reserves the right to refuse the use of personal technology devices depending upon their use and compatibility with the District's network security. Examples of personal technology that will not be allowed on the network include, but are not limited to, personal laptops, printers (wired or wireless), "listening devices" such as Amazon Alexa and Google Home, and wireless access points that circumvent the district network. It is the user's responsibility to request permission to use any personally owned device on the network and to comply with the terms of the Personal Technology Procedure – 6:235 AP1: E7.
3. Inappropriate communication includes, but is not limited to, the following: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted, or spoken by students; information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others; knowingly or recklessly posting false or defamatory information about a person or organization; and communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices. If a student is instructed to stop sending communications, they must cease the activity immediately.
4. Please review 6:235-AP1 E:7 for the full procedure on the use of personally owned technology devices.

No Warranties

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District shall not be liable for any damages incurred by the user. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence, user errors, or omissions**. Students and staff are responsible for backup of their personal files.** The District specifically denies any responsibility for the accuracy or quality of information obtained via the Internet.

Indemnification

To the extent permitted by law, the user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of these rules.

Security

Network security is a high priority. If the user identifies a security problem on the network or the Internet, they must notify the system administrator, the building technology facilitator, or the building principal. The problem should not be described or demonstrated to other users. Accounts and passwords should be kept confidential. Users should not use another individual's account. Attempts to log on to the network as a system administrator will result in the cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

As an extra layer of security, all adult accounts provisioned by the District will be required to enforce multi-factor authentication (MFA). The District will provide multiple methods for MFA, including the use of a personal device, personal email account, or QR codes. The use of personal devices for MFA is recommended, but optional, and will not result in any reimbursable expenses for personal devices. Please review 6:235-AP1 E:8 – Password for more details on password security.

Vandalism

Vandalism will result in the cancellation of privileges and may lead to other disciplinary actions. Vandalism is defined as any malicious attempt to harm or destroy hardware or data of another user, the Internet, or any computer system. This includes, but is not limited to, uploading or creating computer viruses, as well as any attempts to disrupt network resources or communication.

Telephone Charges

The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules

Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on district web sites or file servers without explicit written permission.

- For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
- Students and staff engaged in producing Web pages must provide the Building Superintendent (or designee) with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.

- The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.
- The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- Student work may only be published if there is written permission from both the parent/guardian and student.

These rules may be amended to meet the needs of the Districts. Amendments become binding upon posting.

LEGAL REF.: 20 U.S.C. §7131, Elementary and Secondary Education Act.

47 U.S.C. §254(h) and (l), Children's Internet Protection Act.

720 ILCS 135/, Harassing and Obscene Communications Act.

PRESS REVISED: June 2011, July 2016, June 2021, April 2025

CABINET REVIEWED: October 2016, August 2021, September 2022, July 2025, September 2025

ED TECH UPDATED: September 2020, September 2022, September 2025

Section 2: Exhibits and Definitions

The following contains a summary of the associated Exhibits to this procedure: 6:235-AP 1. By accepting the terms and conditions of AUP 6:235 AP1, you also acknowledge and understand the terms and conditions for each of its associated Exhibits and Administrative Procedures.

5:130 AP: Email Retention and Acceptable Use – This Exhibit outlines guidelines for student and employee use of email, including expectations of privacy, proper email use, and procedures related to the federal Freedom of Information Act (FOIA).

6:235 AP2: Web Publishing Guidelines – The Administrative Procedure outlines the responsibility of any District stakeholder publishing content on the District's behalf. This includes content published directly to the District's website, associated social networks, or any online communication.

7:345-AP E2: Student Online Personal Protection Act (SOPPA) - Effective July 1, 2021, Illinois school districts will be required by the Student Online Personal Protection Act (SOPPA) to provide guarantees that student data is protected when used by educational technology companies, and that data is used for educationally beneficial purposes only (**105 ILCS 85**). The following collapsible sections provide information on the specific requirements and how Moline-Coal Valley CUSD 40 is meeting these requirements.

6:235-AP1: Exhibits and Definitions

- **Exhibit 3: Online Privacy Statement**
- **Exhibit 4: Internet Safety** – Procedures for adults and students to practice private and secure use of social networks and sharing guidelines prohibited for District-issued accounts.
- **Exhibit 5: COPPA (Children's Online Privacy Protection Act)** - Specific Federal law for the privacy of student data when provided to external operators
- **Exhibit 6: Student use of Google Workspace for Education** - Specific guidelines per grade level for the safe use of Google Gmail, Calendar, Docs, Drive, and other Google educational services.
- **Exhibit 7: Personal Technology Procedure for Staff and Students** - Procedure for the approval and use of personal technology within the District's network.
- **Exhibit 8: Employee Password Policy (Staff Only)** - Procedure for defining password complexity, prohibited sharing of passwords, and password expiration.
- **Exhibit 9: Social Media and Online Communication Procedure** - Specific guidelines for the safe and legal use of Social Media platforms and District-sanctioned communication applications (i.e., Remind, Hudl, Twitter, Facebook).
- **Exhibit 10: District Issued Device Procedure (Staff Only)** - Specific guidelines and policies for devices issued to staff and students, including acceptable use, ownership, and events of damage/loss/theft.
- Exhibit 11: AUP Acceptance and Signature - REMOVE