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

Instruction

Administrative Procedure - Web Publishing Guidelines

General Requirements

All material published on the District's website must have educational value and/or support the District's guidelines, goals, and policies. Material appropriate for web publishing includes information about the District and its School Board members, agendas, policies, appropriate administrative procedures, Department activities or services, schools, teachers or classes, student projects, and student extracurricular organizations. Personal information not related to education will not be allowed on the District's website.

The District webmaster shall implement a centralized process for review and uploading of material onto the District's website to ensure that, before the material is published, it complies with District policy and procedures. The District webmaster shall supervise the efforts of all staff members responsible for web publishing at each level of District web publishing and, when appropriate, hold in-serve opportunities for those staff members. The staff members responsible for web publishing are identified in these procedures in the section **Different Levels of Web Publication**. The District webmaster shall provide regular feedback and suggestions to the Superintendent regarding these Guidelines.

All content published on the District's website must:

1. Comply with all State and federal law concerning copyright, intellectual property rights, and legal uses of network computers.
2. Comply with Board policies, administrative procedures, these Guidelines, and other District guidelines provided for specific levels of publishing. This specifically includes the Board's *Access to Electronic Networks* policy and the District's procedures on *Acceptable Use of Electronic Networks*.
3. Due to limited storage space and varying network speeds, file sizes must be kept under 50 kilobytes unless the District webmaster approves otherwise.
4. Comply with the publishing expectations listed below.

Material that fails to meet these Guidelines or is in violation of Board policy and/or procedures shall not be published on the District's website. The District reserves the right to remove any material in violation of its policy or procedures. Failure to follow these Guidelines or Board policy and/or procedures may result in loss of privileges, disciplinary action, and/or appropriate legal action.

Publishing Expectations

The following are minimum expectations for all District web pages:

1. The style and presentation of web-published material should be of high quality and

designed for clarity and readability. Material shall not be published in violation of the District's procedures on *Acceptable Use of Electronic Networks*, including material that is defamatory, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, or harassing material that invades the privacy of any individual. Anonymous messages are prohibited.

2. Correct grammar and spelling are expected.
3. All information must be verifiable.
4. Publications must include a statement of copyright when appropriate and indicate that permission has been secured when including copyrighted materials.
5. Publications must identify affiliation with the District, school, and/or department.
6. Widespread use of external links to non-District websites is discouraged, but if used, the external sites must contain appropriate educational materials and information as exclusively determined by the District. Every effort should be made to ensure that all links are operational. Every link to an external website must open a new browser window.
7. Relevant dates are required on all publications, including the date on which the publication was placed on the District's website. Each site should contain the date the page was last updated.
8. All publications must include the District email address of the staff member responsible for the page. This provides a contact person for questions or comments. If a student is a publisher, the sponsoring staff member's email must be included as the responsible person. Only District staff members may act as student sponsors.
9. Use of the District's website for personal or financial gain is prohibited. No commercial or private accounts should be listed on any District web pages.
10. All documents should be previewed on different web browsers, especially Google Chrome, Mozilla Firefox, or Microsoft Internet Explorer, before being posted on the District's website.

For more information about these expectations or other issues related to web publishing, please contact the System Administrator.

Protecting Student and Staff Privacy

Personal information concerning students or staff members, including home addresses and telephone numbers, shall not be published on District web pages.

A student's last name, last name initial, and grade level shall not be published on District web pages. In addition, student records shall not be disclosed. In special circumstances (e.g., where accolades are warranted), the sponsoring staff member should contact the Building Principal who may seek permission from the student's parents/guardians. Web pages shall not display student pictures with a student identified by his or her name unless written parental permission was first granted (e.g., by executing the form *Using a Photograph or Videotape of a Student*). Student

email addresses, whether a personal or District account, shall not be listed on any District web page.

Submitting Material to Be Published

Everyone submitting material for publication on the District's website shall have signed an *Authorization for Electronic Network Access*. Before material is published on the District's website, the author must authorize the District in writing to publish the material unless the District owns the copyright. All material submitted by a teacher or other staff member for publication on the District's website is deemed "work for hire," and the copyright in those works vests in the District. All material submitted for the District's website is subject to treatment as a District-sponsored publication.

Different Levels of Web Publication

The following guidelines provide specific information regarding web publishing at different levels within the District. At each level, a staff member is identified as being responsible for web publishing at that level. This individual's web publishing efforts are supervised by the District webmaster.

District-Level

The District webmaster conducts the District-level web publishing efforts and supervises other levels of web publishing. District-level publishing includes the District's homepage as well as any publishing activities representing the District as a whole, e.g., information about Board meetings, Board policy, and schedules. The District homepage shall have a link to an Online Privacy Statement.

Department-Level

District departments (e.g., Transportation, Personnel, or Curriculum) may publish their own web pages as part of the District's website. The department supervisor or director is ultimately responsible for his or her respective department's web pages but may appoint a staff member as the department's webmaster to fulfill the maintenance, reviewing, and uploading tasks. The department supervisor or director shall keep the District webmaster informed of who is the department webmaster.

The web-published material should coincide with that department's printed material. The District webmaster should be consulted before publishing potentially sensitive material, e.g., school comparisons or student data.

The department front pages should maintain the look and feel of the District homepage – the connection to the District should be obvious. Links to the main website's "home" must be included at the bottom of the main pages, and the District's logo must be included at the top of the main front pages of each department.

School-Level

The Building Principal is ultimately responsible for his or her respective school's webpages but may appoint a staff member as the school webmaster to fulfill the maintenance, reviewing, and

uploading tasks. The Building Principal shall keep the District webmaster informed of who is the school webmaster. All official material originating from the school will be consistent with the District style and content guidelines. The Building Principal or school webmaster may develop guidelines for the various sections of and contributors to the school's web pages.

Staff-Level

Any teacher or other staff member wanting to create web pages for use in class activities or to provide a resource for other teachers or staff members shall notify the school webmaster of his or her desired publishing activities.

Student-Level

A student wanting to create web pages on the District's website as part of a class or school-sponsored activity should request a teacher or staff member to sponsor the student's publishing efforts. The sponsoring teacher or staff member shall notify the school webmaster of the desired publishing activities. The student's web page must include an introduction written by the sponsor that describes the intent of the student's web page and contains the sponsor's District email address. Student web pages will be removed at the end of the school year unless special arrangements are made.

Personal web pages are not allowed on the School District's web server. Likewise, student web pages may not contain commercial or advertising links, including links to games and advertisements for games.

CROSS REF.:	6:235 (Access to Electronic Networks) 7:315 (Restrictions on Publications; High Schools)
ADMIN. PROC.:	5:170-AP1 (Copyright Compliance) 6:235-AP1 (Acceptable Use of the District's Electronic Networks) 6:235-AP1, E1 (Student Authorization for Access to the District's Electronic Networks) 6:235-AP1, E2 (Staff Authorization for Access to the District's Electronic Networks) 6:235-E3 (Online Privacy Statement)
PRESS REVISED:	October 2012, July 2016, June 2021
CABINET REVIEWED:	October 2016, August 2021, September 2022

Instruction

Exhibit - Online Privacy Statement

Online Privacy Statement
The School District respects the privacy of all website visitors to the extent permitted by law. This Online Privacy Statement is intended to inform you of how this website collects information, the uses to which that information will be put, and how we will protect any information you choose to provide us.

There are four types of information that this site may collect during your visit: network traffic logs, website visit logs, cookies, and information voluntarily provided by you.

Network Traffic Logs
In the course of ensuring network security and consistent service for all users, the District employs software programs to do such things as monitor network traffic, identify unauthorized access or access to nonpublic information, and detect computer viruses and other software that might damage District computers or the network, and monitor and tune the performance of the District network. In the course of such monitoring, these programs may detect such information as e-mail headers, addresses from network packets, and other information. Information from these activities is used only to maintain the security and performance of the District's networks and computer systems. Personally identifiable information from these activities is not released to external parties without your consent unless required by law.

Website Visit Logs
The District routinely collects and stores information from online visitors to help manage those sites and improve service. This information includes the pages visited on the site, the date and time of the visit, the Internet address (URL or IP address) of the referring site (often called "referrers"), the domain name and IP address from which the access occurred, the version of browser used, the capabilities of the browser, and search terms used on our search engines. This site does not attempt to identify individual visitors from this information; any personally identifiable information is not released to external parties without your consent unless required by law.

Cookies
Cookies are pieces of information stored by your web browser on behalf of a website and returned to the website on request. This site may use cookies for two purposes: to carry data about your current session at the site from one webpage to the next and to identify you to the site between visits. If you prefer not to receive cookies, you may turn them off in your browser or may set your browser to ask you before accepting a new cookie. Some pages may not function properly if the cookies are turned off. Unless otherwise notified on this site, we will not store data, other than for these two purposes, in cookies. Cookies remain on the District computer, and accordingly, we neither store cookies on our computers nor forward them to any external parties. We do not use cookies to track your movement among different websites and do not exchange cookies with other entities.

Information Voluntarily Provided by You

In the course of using this website, you may choose to provide us with information to help us serve your needs. For example, you may send us an email to request information, an application, or other material, and you may sign up for a mailing list. Any personally identifiable information you send us will be used only for the purpose indicated. Requests for information will be directed to the appropriate staff and may be recorded to help us update our site. We will not sell, exchange, or otherwise distribute your personally identifiable information without your consent, except to the extent required by law. We do not retain the information longer than necessary for normal operations.

Each webpage requesting information discloses the purpose of that information. If you do not wish to have the information used in that manner, you are not required to provide it. Please contact the person listed on the specific page or listed below with questions or concerns about the use of personally identifiable information.

While no system can provide guaranteed security, we make reasonable efforts to keep the information you provide to us secure, including encryption technology (if any) and physical security at the location of the server where the information is stored.

Communication Preferences

You can stop the delivery of informational emails from the District by following the specific instructions in the email you receive. Depending on the respective service, you may also have the option of proactively making choices about the receipt of the email, telephone calls, and postal mail for particular District information and activities.

Links to Non-District Websites

District websites provide links to other websites or resources. We do not control these sites and resources, do not endorse them, and are not responsible for their availability, content, or delivery of services. In particular, external sites are not bound by this Online Privacy Statement; they may have their own policies or none at all. Often you can tell you are leaving a District website by noting the URL of the destination site. These links to external websites open a new browser window as well.

Please email your questions or concerns to the Director for Technology, Craig Reid, at *creid@molineschools.org*.

PRESS REVISED: July 2013, July 2016, June 2021

CABINET REVIEWED: October 2016, August 2021, September 2022

Instruction

Exhibit - Keeping Yourself and Your Kids Safe On Social Networks

For students:

- Put everything behind password-protected walls, where only friends can see.
- Protect your password and make sure you really know who someone is before you allow them onto your friend list.
- Blur or morph your photos a bit so they won't be abused by cyberbullies or predators.
- Don't post anything your parents, principal, or a predator couldn't see.
- What you post online stays online - forever!!!! So ThinkB4UClick!
- Don't do or say anything online you wouldn't say offline.
- Protect your privacy and your friend's privacy, too. Get their okay before posting something about them or their likeness online.
- Check what your friends are posting/saying about you. Even if you are careful, they may not be and may be putting you at risk.
- That cute 14-year-old boy may not be cute, may not be 14, and may not be a boy! You never know!
- And, unless you're prepared to attach your blog to your college/job/internship/scholarship or sports team application…don't post it publicly!
- Stop, Block, and Tell! (don't respond to any cyberbullying message, block the person sending it to you and tell a trusted adult).
- R-E-S-P-E-C-T! (use good netiquette and respect the feelings and bandwidth of others).
- Keep personal information private (the more information someone has about you, the more easily they can bully you).
- Google yourself! (conduct frequent searches for your own personal information online and set alerts … to spot cyberbullying early).
- Take 5! (walk away from the computer for 5 minutes when something upsets you, so you don't do something you will later regret).

And for parents:

- Talk to your kids - ask questions (and then confirm to make sure they are telling you the truth!)
- Ask to see their profile page (for the first time) …tomorrow! (It gives them a chance to remove everything that isn't appropriate or safe…and it becomes a way to teach them what not to post instead of being a gotcha moment! Think of it as the loud announcement before walking down-stairs to a teen party you're hosting.)
- Don't panic…there are ways of keeping your kids safe online. It's easier than you think!
- Be involved and work with others in your community. (Think about joining WiredSafety.org and help create a local cyber-neighborhood watch program in your community.)
- Remember what you did that your parents would have killed you had they known when you were fifteen.

- This, too, will pass! Most kids really do use social networks just to communicate with their friends. Take a breath, gather your thoughts and get help when you need it. (You can reach out to WiredSafety.org.)

*Ed Tech has modified the procedure to align with the Moline-Coal Valley School District policies

- It's not an invasion of their privacy if strangers can see it. There is a difference between reading their paper diary that is tucked away in their sock drawer…and reading their blog. One is between them and the paper it's written on; the other is between them and 700 million people online!
- Don't believe everything you read online - especially if your teen posts it on her blog!

For more information, visit www.WiredSafety.org; https://www.stopbullying.gov/.

Reprinted with permission from "Parry Aftab's Guide to Keeping Your Kids Safe Online, Facebook, Twitter, and Xanga, Oh! My!" Parry Aftab, Esq., www.aftab.com.

Resources for Students and Parents

Resources for students:

Federal Trade Commission - Kids and Socializing Online www.onguardonline.gov/articles/0012-kids-and-socializing-online.

National Center for Missing and Exploited Children – Teens Talk Back, Social Networking www.netsmartz.org/TeensTalkBack/SocialNetworking.

Resources for parents:

National Crime Prevention Council – Social Networking Safety, Tips for Parents www.ncpc.org/topics/internet-safety/social-networking-safety. A great comprehensive article for parents.

National Cyber Security Alliance - Raising Digital Citizens.

Illinois Attorney General – Stay Connected Stay Informed www.illinoisattorneygeneral.gov/cyber-bullying/.

DHS U.S. CERT - Socializing Securely: Using Social Networking Services www.us-cert.gov/sites/default/files/publications/safe_social_networking.pdf.

DHS U.S Computer Emergency Readiness Team - Staying Safe on Social Network Sites www.us-cert.gov/ncas/tips/ST06-003 (January 26, 2011).

Internet Safety: Social Networking Sites for Children blog.privatewifi.com/internet-safety-social-networking-sites-for-children/ (March 30, 2011).

8 Safe Social Networks for Kids kommein.com/8-safe-social-networks-for-kids/ (Jan. 5, 2011).

PRESS REVISED: June 2011, July 2016, June 2021

CABINT REVIEWED: October 2016, August 2021, September 2022

ED TECH UPDATED: September 2022

*Ed Tech has modified the procedure to align with the Moline-Coal Valley School District policies

Instruction

Exhibit - Children's Online Privacy Protection Act

Dear Parent(s)/Guardian(s):

This procedure is part of the District's continuing effort to educate parents and students about privacy protection and Internet use.

The Children's Online Privacy Protection Act gives parents control over what information websites can collect from their children. Many companies, however, are not providing information about what data a mobile app collects, who will have access to that data, and how it will be used. Allowing your child access to games and other seemingly harmless applications on a smartphone or computer risks his or her exposure to intrusive marketing and access to personal information.

A recent survey of apps for children by the Federal Trade Commission found that 10 percent of apps with social networking services did not disclose their presence; 17 percent of the apps allowed children to make purchases without parent/guardian consent; and 58 percent contained constant advertising, while less than 20 percent disclosed that advertising would appear.

The following suggestions may help keep children from being bombarded by unwanted advertising, from making unwanted purchases, and from disclosing personal information and location:

- Be choosy about the applications that you let your child use. Try the app yourself to check for advertising messages and/or social networking and purchase options before allowing your child access.
- Select activities that do not require access to the Internet or an application, such as looking at family pictures or listening to preselected music, screened and approved by you.
- Make certain that the ability to make purchases is password protected.
- Set up family rules and consequences explaining that all purchases made via a smartphone or computer must have parent/guardian consent.
- Caution children about the use of social networking and other sites and/or apps that can pinpoint locations.
- Monitor computer and smartphone use whenever and wherever possible.

For more information on the Children's Online Privacy Protection Act, please see the following links:

www.ftc.gov/opa/2012/12/kidsapp.shtm

https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

PRESS REVISED: March 2013, June 2016

CABINET REVIEWED: June 2016, November 2020, September 2022

Instruction

Exhibit – Google Apps for Education Permission Form

Dear Parents/Guardians,

The Moline-Coal Valley School District provides all students, teachers and staff with Google Apps for Education accounts, a free web-based program for word processing, spreadsheet, presentation and web authoring tools. Google Apps for Education also includes a password-protected email account for school use only.

Google Apps for Education runs on an Internet domain purchased and owned by the Moline School District and is intended for educational use only. This permission form describes the responsibilities of the school, students, and parents in using Google Apps for Education on the District's domain in accordance with District policies and procedures outlined in the Acceptable Use Policy.

As with any educational endeavor, a strong partnership with families is essential to a successful experience.

The following services are available to each student and hosted by Google as part of Moline School District's online presence in Google Apps for Education:

Mail - an individual email account for school use managed by the Moline School District

- Grades K-2 do not have any access to email
- Grades 3-5 can only send/receive email to/from specific teachers and Principals within the Moline School District
- Grades 6-10 cannot send/receive any email from outside the Moline School District domain (only addresses containing @molineschools.org are allowed)
- Grades 11-12 are not restricted

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

- Available for all grade levels

Drive - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

- Available for all grade levels

Sites - an individual and collaborative website creation tool

- Available for all grade levels

Classroom – A learning management system for course instruction and instructional materials.

- Available for all grade levels

Using these tools, students collaboratively create, edit and share files and websites for school related projects and communicate via email and/or drive with other students and teachers. These services are

entirely online and available 24/7 from any Internet-connected computer or mobile device. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

Technology use in the Moline-Coal Valley School District is governed by federal laws including:

Children's Online Privacy Protection Act (COPPA)

COPPA applies to commercial companies and limits their ability to collect personal information from children under

13. By default, advertising is turned off for Moline School District's presence in Google Apps for Education. No personal student information is collected for commercial purposes. This permission form allows the school to act as an agent for parents in the collection of information within the school context. The school's use of student information is solely for education purposes.

--COPPA – http://www.ftc.gov/privacy/coppafaqs.shtm

Family Educational Rights and Privacy Act (FERPA)

FERPA protects the privacy of student education records and gives parents the rights to review student records. Under FERPA, schools may disclose directory information (See Board Policy JOA) but parents may request the school not disclose this information. Parents are provided the opportunity annually to opt out of disclosing their student's directory information on the District's Enrollment Form.

--FERPA – http://www.ed.gov/policy/gen/guid/fpco/ferpa

Student Online Privacy Protection Act (SOPPA)

SOPPA is a school law that requires the District to enter into a signed agreement with educational technology partners that guarantees providers do not sell student personal data they collect and that their services are for educational use only.

--SOPPA – https://www.ilga.gov/legistlation/ilcs/ilcs3.asp?ActID=3806&ChapterID=17

Guidelines for the responsible use of Google Apps for Education by students:

1. **Official Email Address.** All students will be assigned a username@molineschools.org email account. This account will be considered the student's official Moline-Coal Valley School District email address until such time as the student is no longer enrolled with the Moline-Coal Valley School District.

2. **Prohibited Conduct.** Please refer to the Board Policy 6:235, 7:180, District Procedure 6:235-AP1 and 6:235-AP2.

3. **Access Restriction.** Access to and use of student email is considered a privilege accorded at the discretion of the Moline-Coal Valley School District. The District maintains the right to immediately withdraw the access and use of these services including email when there is reason to believe that violations of law or District policies have occurred. In such cases, the alleged violation will be referred to a building Administrator for further investigation and adjudication.

4. **Security.** Moline-Coal Valley School District cannot and does not guarantee the security of

electronic files located on Google systems. Although Google does have a powerful content filter in place for email, the District cannot assure that users will not be exposed to unsolicited information.

5. **Privacy.** The general right of privacy will be extended to the extent possible in the electronic environment. Moline-Coal Valley School District and all electronic users should treat electronically stored information in individuals' files as confidential and private. However, users of student email are strictly prohibited from accessing files and information other than their own. The District reserves the right to access any student's Google account, including current and archival files of user accounts when there is reasonable suspicion that unacceptable use has occurred.

6. **Notice Regarding Third-Party Apps.** The District allows students to access additional third-party services with their Google Workspace for Education accounts. The Educational Technology Department enables access to these third-party services with your student's Google account, and authorizes the disclosure of data, as requested by the third-party services. Data that approved third-party services may access includes:

    - Activity while using additional services, which includes items such as terms your student searches for, videos they watch, content and ads they view and interact with, voice and audio information when they use audio features, purchase activity, and activity on third-party sites and apps that us Google services.
    - apps, browsers, and devices. Google collects the information about your student's apps, browser, and devices described above in the core services section.
    - location information. Google collects info about your student's location as determined by various technologies including GPS, IP address, sensor data from their device, and information about things near their device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices. The types of location data we collect depend in part on your student's device and account settings.

Be agreeing to this Acceptable Use Policy, you are granting permission for your student to utilize their Google Workspace for Education account to access approved third-party services that meet the District's criteria for acceptable educational use.

Google Workspace for Education Granted Permission as Part of the Acceptable Use Policy:

By accepting this AUP in its entirety, I confirm that I have read and understand the following:

-Under FERPA, COPPA, and SOPPA and all corresponding Illinois or federal law, a student's education records are protected from disclosure to third parties.

-I understand that my student's Google Workspace for Education account may be used to access approved third-party services to gain access to these services for educational purposes.

-I understand that my student's education records stored in Google Workspace for Education may be accessible to someone other than my student and the Moline-Coal Valley School District by virtue of this online environment. My acceptance in this registration step confirms my consent to storing my student's education record by Google.

I understand that by participating in Google Workspace for Education, information about my child will be collected and stored electronically. I have read the privacy policies associated with use of Google Workspace for Education (http:// www.google.com/a/help/intl/en/edu/privacy.html). I understand that I may ask for my child's account to be removed at any time.

_____ **YES**, I give permission for my child to be assigned a full Moline School District Google Workspace for Education account. This means my child will receive an email account, access to Google Docs, Calendar, and Sites.

_____ **NO**, I do not give permission for my child to be assigned a full Moline School District Google Workspace for Education account. This means my child will NOT receive an email account or access to Docs, Calendar, and Sites.

Student Name (Print): _____

Student ID # (if known): _____ Grade: _____

Parent/Guardian Signature: _____ Date: _____

Please sign and return this form for each student with the rest of the enrollment packet.

Instruction

Exhibit - Personal Technology Procedure

General Purpose:
The District adopts this policy in order to maintain a safe and secure environment for students and employees using personal technology within the District.

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 acceptable personally owned device shall include but is not limited to: streaming media players, tablet devices, cell phones, and smart phones, as well as any device with similar capabilities.

Personal devices that will not be allowed to connect to the network include laptops (Mac or PC), Chromebooks and netbook computers, personally owned or purchased printers (wired or wireless), wireless streaming devices, "listening" devices such as Amazon Alexa and Google Home, and any device used to provide a wireless network used to circumvent the District's production network.

Inappropriate Use:
Inappropriate use of personal technology includes, but is not limited to the following: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images; 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.

Reinforcement:
Failure to adhere to this procedure could result in disciplinary measures commensurate with the infraction, school code, and District policy.

General Procedure for Employees and Students:

1) Personal devices used within the District are used at the risk of employees, students, and guardians. The District is not responsible for any damage, loss, theft, financial loss or data loss that occurs during the use of the personal device.

2) The use of personal technology is solely limited to supporting and enhancing instructional activities currently occurring in the classroom environment or within specific district roles.

3) Connecting personal technology to the District's Guest network may not be successful if the technical specifications for wireless protocol are not met. The District will not provide technical support above and beyond basic connectivity for any personal device.

4) No personal technology may be attached to the District production wireless or physical network.

5) No employee or student shall establish a wireless ad-hoc or peer-to-peer network using his/her electronic device or any other wireless device while on school grounds. This includes but is not limited to using a privately owned electronic device as a cabled or wireless hotspot.

6) Employees and students who bring personal technology into the District do so knowing that it will give up their expectation of privacy regarding their personal electronic devices while at school. The District reserves the right to search a privately owned electronic device in accordance with applicable laws and policies if there is reasonable suspicion that the employee or student has violated Moline-Coal Valley School District policies, administrative procedures, and school rules or engaged in other misconduct while using the personal device.

7) No personal technology should ever be connected by cable to the Moline-Coal Valley School District network. Network access is provided via a wireless connection to the Guest network only. Access to the District's production network must be explicitly granted by the Educational Technology Department.

8) No district-owned academic or productivity software can be installed on personal devices.

General Procedure (Students Only):

1) Teacher permission is necessary for student use of a privately owned electronic device during classroom instruction or the classroom period.

2) Students are not to call, text message, email, or electronically communicate with others from their personal devices, including other students, parents, guardians, friends, and family, during the school day unless given explicit permission by a teacher or District Administrator.

3) Students are prohibited from accessing the Internet using their cellular network provider. i.e.: Verizon, Sprint, AT&T, US Cellular, etc.

4) Voice, video, and image capture applications may only be used with teacher permission and for specific instructional purpose(s). All Administrative Procedures within the Acceptable Use Policy (6:235) must be followed.

5) The teacher may request at any time that privately owned electronic devices be turned off and put away. Failure to do so may result in disciplinary action and revocation of access to the network.

6) Sound should be muted unless the teacher grants permission for use of sound associated with the instructional activities.

7) The district advises that privately owned electronic devices be used by the owner and not shared.

8) Students will only use appropriate educational applications on their device (i.e. not games and/or non- school-related tasks and functions).

9) The district Internet connection is filtered using commercial filtering software that will block categories such as; pornography, gambling, social networking, non-educational games, peer-to-peer networking, and custom URLs. The district uses this software to report Internet activities for any filtered computer.

10) No student shall use any computer or device to illegally collect any electronic data or disrupt networking services. Students may not engage in any malicious use, disruption, or harm to the school network, Internet services, learning environment, or any other electronic device owned by the school, any school personnel, and/or student.

11) Students may not attempt to use any software, utilities, or other means to access Internet sites or content blocked by school district Internet filters.

12) Classroom teachers will request parent/guardian signatures for any use of personal technology in their classroom as part of the Full AUP (See Exhibit 11 for signing page).

CABINET REVIEWED: September 2020, September 2022

Moline-Coal Valley Community Unit School District Procedure (Not in PRESS)
*Ed Tech has modified the procedure to align with the Moline-Coal Valley School District policies

Instruction

Exhibit - Password

Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password and a password that does not expire may result in the compromise of Moline-Coal Valley School District's (District hereafter) entire network. It could also lead to the compromise of staff's personal, financial and professional data. As such, all adult District computer users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. All adult users will be required to change their password at designated times during the school year (TBD).

Scope

This procedure applies to all adult employees of the Moline-Coal Valley School District who have any form of computer or application account that requires password access. Examples of accounts include, but are not limited to:

- Employee workstation (desktop, laptop, tablet, Macintosh or Windows)
- Network account login
- Email
- Centralized applications (Google, Employee Portal, Student Information System)

Password Policy

General Password Guidelines

1. Passwords should not be based on well-known or easily accessible information, including personal information.
2. Moline-Coal Valley School District's centralized directory will be used to ensure that passwords meet complexity requirements as outlined below.
3. Passwords should never be shared with any other individual or group under any circumstance. Voluntarily giving password information is a direct violation of the AUP, and disciplinary action may be taken.
4. Passwords should never be written down or displayed in plain view.
5. Passwords should never be re-used. The district's centralized directory will ensure that passwords remain unique.

Moline-Coal Valley School District Password Complexity Requirements

1. Passwords are at least 8 characters long and no longer than 12 characters.
2. Passwords contain at least one upper case letter.
3. Passwords contain at least 4 numbers.

4. Passwords may not be re-used.
5. Example 1: Abcd2345

Password Protection Guidelines

1. Passwords are to be treated as confidential at all times. Under no circumstances is an employee to provide password information to another person. This includes never providing passwords to EdTech staff, Administrators, substitute teachers, student teachers, students, friends, or family. Doing so directly compromises confidential data, financial information and electronic communication.
2. Under no circumstances will any member of the Moline-Coal Valley School District (including EdTech) request a password in any electronic form. Passwords should never be shared via email, forms, or over the phone.
3. EdTech may request an employee password for troubleshooting only and only in person. Once the issue is resolved, EdTech will reset the user's password and force it to be changed again.
4. Do not use the "Remember Password" feature within online applications.
5. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the EdTech Department immediately. EdTech will reset the password and force a new password at the next login.
6. If EdTech successfully guesses or cracks a password as part of its security audits, the user will be required to change the password regardless of the password age.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action.

CABINET REVIEWED: September 2020, September 2022

Instruction

Exhibit - Online Communication and Social Media Procedure

Purpose

Online communication and social media offer (referred to as "online channels" in this procedure) a means by which the Moline-Coal Valley School District (referred to as "District") can quickly communicate, share information, and exchange ideas with district stakeholders, parents, guardians, staff and students. This procedure outlines the behaviors and guidelines that anyone representing the Moline-Coal Valley School District within online channels is expected to follow. This may include:

- Personal use of social media (i.e. Twitter, Facebook, Instagram) that references the District, its students, staff, or Board of Education
- Directed use of social media, either as a district volunteer, district-appointed personnel, or community member representing the District
- Any communication using online channels, such as Remind, SkyAlert, E-Mail, or Web Publishing
- Classroom use of these tools, whether hosted by the District or within the public domain
- District use of these tools as appointed by the Superintendent's office

Social Media Account Approval Guidelines and Process

1. Requests to represent the District or create a social media account on behalf of the MCV must be done online via the Social Media Approval Application <http://bit.ly/mcv-socialmedia-request>. All information on this form must be completed.
    - Applications will be reviewed, and applicants will be notified if denied or approved.
    - Decisions to approve or deny are made by central administration.
2. Anyone representing the District MUST have a signed copy of this procedure AND the full 6:235 Acceptable Use Policy on file with HR before using or creating an online channel.
3. If approved, the applicant will be required to complete online training for appropriate use of Social Media and Online Communication and renew that training annually. Failure to complete the online training will result in the account being removed.
4. The district requires that a secondary administrator account is added or primary account credentials are shared if the originator is no longer filling the same role or this procedure is violated. Upon approval, instructions will be provided.
5. Approval of the application is only for district-approved Social Media channels, such as Facebook and Twitter. Any online communication outside of these channels is prohibited. See the Guidelines below for acceptable and non-acceptable use.

Guidelines for Best Practice

Online communication and social media can blur the lines between what is public or private, personal and professional. The following guidelines must be followed whenever representing the Moline-Coal Valley School District in social media or online communication and applies to community affiliates, staff, and students.

1. Always comply with any Board of Education Policies including, but not limited to:
    - Personal Technology and Social Media; Usage and Conduct – 5:125
    - Sexual Harassment – 5:10

- Student Records – 5:150 and 7:340
- Student and Family Privacy Rights – 7:15
- Student Rights and Responsibilities – 7:130
- Preventing Bullying, Intimidation and Harassment – 7:180
- Employee Student Relations – 5:121
- Acceptable Use Policy – AP1 6:235
- Mandatory Reporting of Suspected Abuse or Neglect – 5:90
- Copyright – 5:170
- Student Online Privacy Protection Act (SOPPA) –7:345

2. Use good judgment in all situations
3. Regardless of your privacy settings, assume that all of the information you have shared within online channels is public information
4. Be respectful
    - Always treat others in a respectful, positive and considerate manner
    - Never degrade the District, its students, staff, or Board of Education
5. Be responsible and ethical
    - Be open about your affiliation with the school/District and the role/position you hold
    - Make sure you understand the information being shared and the possible repercussions

Never share the following:

1. Confidential Information
    - Do not publish, post or release information that is considered confidential. Online "conversations" are never private. Take caution in posting personally identifiable information on a public website, such as your birth date, cell phone, and address.
2. Private and personal information
    - To ensure your safety, be careful about the type and amount of personal information you provide. Avoid publishing personal schedules or situations.
    - NEVER give out or transmit personal information of students, parents, or co-workers
    - Always respect the privacy of the school's community members, families, and students.
    - NEVER use direct messaging within a Social Media channel. For example, do not communicate directly with staff or students using Facebook Messenger, Twitter, Instagram Direct Messaging, or Snapchat.

Use caution with respect to:

- Images
    - Respect brand, trademark, copyright information, and/or images of district property
    - It is generally not acceptable to post pictures of students without expressed written consent of their legal guardian
    - Immediately remove a post if a student's parent/guardian requests it
- Terms and conditions of the social media system
    - A significant part of the interaction on blogs, Twitter, Facebook, and other social media involves passing on interesting content or linking to helpful resources. The poster is ultimately responsible for any content that is shared.
        - Do not blindly repost a link without looking at the content first
- When using Twitter, Facebook, and other online channels, be sure to follow their printed terms and conditions

- Pay attention to the security warnings that pop up on your computer before clicking on unfamiliar links. They actually serve a purpose and protect you and the school

Ensure the integrity of the information being shared:

1. Be sure to correct any mistake immediately
2. Apologize for the mistake when appropriate
3. Report any major mistake (i.e. exposing private information or reporting confidential information) to the Superintendent's office immediately
4. Always follow correct Netiquette rules
    - Users should always be courteous and respectful manner when using social media
    - Users should always recognize that amongst the valuable content online, there may be unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.
5. Users should remember not to post anything online that they wouldn't want parents, teachers, future colleges, or employers to see.

Personal Safety

If you see a message, comment, image, or anything that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

- Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission
- Users should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.
Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained by others. Personal social media accounts ***are not*** exempt from this procedure.

Examples of Acceptable Use

This is not intended to be an exhaustive list. Users should use their own good judgment when using social media.

I will:

- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline
- Treat social media and online communication carefully, and alert staff if there is any problem with their operation
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies
-

- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online
- Be cautious to protect the safety of myself and others
- Only use approved Social Media channels and online communication tools that are approved by the District (i.e. Facebook, Twitter, Remind, Hulu).

Examples of Unacceptable Use

This is not intended to be an exhaustive list. Users should use their own good judgment when using social media.

I will **not**:

- Use social media in a way that could be personally or physically harmful to me or others
- Use direct messaging applications with students, staff, or the community (i.e. direct messages from Twitter or Instagram, Snapchat, and Facebook Messenger).
- Engage in cyberbullying, harassment, or disrespectful conduct toward others--staff or students
- Use language online that would be unacceptable in the classroom
- Degrade or negatively portray the District, its students, staff, or Board of Education

Violations of this Social Media and Online Communication Procedure

Violations of this procedure may have disciplinary repercussions, including, but not limited to:

- Suspension of volunteer privileges
- Removal from positions of leadership within Moline-Coal Valley Schools
- Removal of a student from Moline-Coal Valley Schools
- Additional consequences determined by Administration and/or Board of Education.

CABINET REVIEWED: September 2020, November 2020, September 2022

Instruction

Exhibit – District-Issued Device Agreement

Purpose
Employees that are issued a device will be required to agree to the terms of use as outlined in this procedure. It is the responsibility of the employee to ensure the issued device is cared for in a manner reflective of the District's investment.

1. I understand that the device is the property of the District, and my use of the device is subject to the rules and procedures contained in the District's Acceptable Use Policy (6:235AP1, 6:235AP2, Exhibits 1-10). These policies, procedures, and exhibits can be found at http://bit.ly/mcv-techpolicy.
2. I understand I am being issued a device to facilitate student instruction and enhance student achievement; it will be in my possession for use at school. It may also be in my possession for school use away from school. If not able to be in my possession, it will be locked and secured.
3. I understand that the device and all accessories will be returned to the District's Educational Technology Office immediately upon termination of my employment or at any time specifically directed by District authority.
4. I understand that in the event of damage, loss, or theft of the laptop, I will immediately notify my building administrator AND the Educational Technology Department. In the case of theft, I will file a report with the police department and provide all documentation to District administration.
5. I understand that I am required to report any instance of damage to the device, regardless of circumstance, to the Educational Technology Department. I may not use a third-party repair service or self-repair the laptop.
6. I understand that the District will assess any circumstance of total device loss due to my intentional act or negligence, and I may be responsible for device costs if determined I failed to adhere to these guidelines or the Acceptable Use Policy. Further, I understand that the replacement cost will be based on the following fee schedule:
    a. 1st year – 100% of purchase price
    b. 2nd year – 75% of purchase price
    c. 3rd year – 50% of purchase price
    d. 4th year – 25% of purchase price
7. I understand that I may not make any marks or use stickers on my device that are not easily removed.
8. I understand that it is my responsibility to make sure ALL files are backed up to my Google Drive folder. Further, I understand that the District is not responsible for any loss of data stored on the laptop.
9. I understand the following guidelines are recommended and expected to ensure the device's longevity:
    a. Any updates OR new software installations should be performed by EdTech.
    b. The device should never be left unattended in any unlocked area, i.e. classroom, instructional area, office, vehicle, or common area.
    c. The device should not be shared with anyone else, i.e. substitutes, paraprofessionals and students.
    d. Never expose the device to extremely hot or cold environments for long periods.
    e. Report to EdTech any issues immediately.

CABINET REVIEWED: September 2020, November 2020, September 2022

Instruction

Summary and Acceptance of the Terms Contained with the Acceptable Use Policy

This is a summary of the full Acceptable Use Policy (AUP) and all Exhibits. Signing this summary page is a receipt of acceptance of the terms and conditions within the entire AUP.

1. Administrative Procedure 5:130: General Personnel
    a. District data, including email, attachments, cloud storage, and any other electronic communication or files, are subject to inspection as per the Freedom of Information Act and are the property of the Moline-Coal Valley CUSD 40.
2. Administrative Procedure 6:235 AP1: Access to Electronic Network
    a. Defines acceptable use of the District's electronic network to support educational purposes, including proper use of email, cloud storage, the District's phone system, and web publishing guidelines.
3. 6:235 Exhibit 3: Online Privacy Statement
    a. Defines the District's policy for published resources for hosted websites either internally or through 3rd party affiliates (i.e. Google Site, blogs, vlogs).
4. 6:235 Exhibit 4: Keeping Yourself and Your Students Safe on Social Networks
    a. Procedures for adults and students to practice private and secure use of social networks (i.e., Twitter and Facebook) and sharing guidelines prohibited with district accounts.
5. 6:235 Exhibit 5: Children's Online Privacy Protection Act (COPPA)
    a. Specific Federal law for the privacy of student data when provided to external operators
6. 6:235 Exhibit 6: Google for Education Permission Form
    a. Specific guidelines per grade level for the safe use of Google Gmail, Calendar, Docs, Drive, and other Google educational services.
7. 6:235 Exhibit 7: Personal Technology Procedure
    a. Procedure for the approval and use of personal technology within the District's network.
8. 6:235 Exhibit 8: Password Procedure
    a. Procedure for defining password complexity, prohibited sharing of passwords, and password expiration.
9. 6:235 Exhibit 9: Online Communication and Social Media Procedure
    a. Specific guidelines for the safe and legal use of Social Media platforms and District-sanctioned communication applications (i.e., Remind, Hudl, Twitter, Facebook).
10. 6:235 Exhibit 10: District-Issued Device Agreement
    a. Specific guidelines and policies for devices issued to staff and students, including acceptable use, ownership, and events of damage/loss/theft.

I have read and understand this Acceptable Use Policy with all Exhibits and agree to abide by it:

_____ _____
(Signature) (Date)

_____ _____
(Printed Name) (District position, role, affiliate)

ADOPTED: May 2021

CABINET REVIEWED: May 2021, September 2022

Students

Exhibit – Student Data Privacy; Notice to Parents About Educational Technology Vendors

Use the sample text below to provide notice to parents/guardians about educational technology vendors pursuant to the Student Online Personal Protection Act, 105 ILCS 85/28(e), added by P.A. 101-516, eff. 7-1-21. Beginning with the 2021-2022 school year, school districts must provide this notice to parents/guardians at the beginning of each school year through distribution of school handbooks or other means generally used by a district to provide such notices to parents/guardians.

Annual Notice to Parents about Educational Technology Vendors Under the Student Online Personal Protection Act

School districts throughout the State of Illinois contract with different educational technology vendors for beneficial K-12 purposes such as providing personalized learning and innovative educational technologies, and increasing efficiency in school operations.

Under Illinois' Student Online Personal Protection Act, or SOPPA (105 ILCS 85/), educational technology vendors and other entities that operate Internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes are referred to in SOPPA as *operators*. SOPPA is intended to ensure that student data collected by operators is protected, and it requires those vendors, as well as school districts and the Ill. State Board of Education, to take a number of actions to protect online student data.

Depending upon the particular educational technology being used, our District may need to collect different types of student data, which is then shared with educational technology vendors through their online sites, services, and/or applications. Under SOPPA, educational technology vendors are prohibited from selling or renting a student's information or from engaging in targeted advertising using a student's information. Such vendors may only disclose student data for K-12 school purposes and other limited purposes permitted under the law.

In general terms, the types of student data that may be collected and shared include personally identifiable information (PII) about students or information that can be linked to PII about students, such as:

- Basic identifying information, including student or parent/guardian name and student or parent/guardian contact information, username/password, student ID number
- Demographic information
- Enrollment information
- Assessment data, grades, and transcripts
- Attendance and class schedule
- Academic/extracurricular activities
- Special indicators (e.g., disability information, English language learner, free/reduced meals or homeless/foster care status)
- Conduct/behavioral data
- Health information
- Food purchases
- Transportation information

- In-application performance data
- Student-generated work
- Online communications
- Application metadata and application use statistics
- Permanent and temporary school student record information

Operators may collect and use student data only for K-12 purposes, which are purposes that aid in the administration of school activities, such as:

- Instruction in the classroom or at home (including remote learning)
- Administrative activities
- Collaboration between students, school personnel, and/or parents/guardians
- Other activities that are for the use and benefit of the school district

ADOPTED: June 2020

PRESS REVISED:

CABINET REVIEWED: October 2020