

Instruction

Administrative Procedure - Acceptable Use of the District's Electronic Network

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow the *Access to Electronic Network Policy*, these procedures, or any other rules promulgated by the Superintendent or his or her designee(s) will result in the loss of privileges, disciplinary action, and/or legal action.**

Terms and Conditions

Authorized Users - Authorized users of the electronic network include students, teachers, administrators, other employees of the District, Board of Education members, and other non-student users who have signed and submitted an *Authorization for Electronic Network Access Form* and whose electronic network privileges are not suspended or revoked.

Acceptable Use - Access to the District's electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use. Access also must comply with the Policy and all other procedures, rules, exhibits or other **terms** or conditions of electronic network access promulgated the Superintendent or his or her designee(s), and all other disciplinary policies and regulations necessary for the safety and pedagogical concerns of the District.

Privileges - The use of the District's electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges, disciplinary action, and/or appropriate legal action. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final. Revocation of network access will limit the student's ability to access instructional resources and the ability for timely online assessments.

Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Any use that is not for the purpose of education, research, or legitimate school business, or that is otherwise inconsistent with the District's educational mission, is an unacceptable use.

Some examples of unacceptable uses are:

- a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
- b. Taking any steps which threaten, or which may reasonably be interpreted to threaten, any person, group of persons, building, or property with harm, regardless of whether the user intends to carry out such threat.
- c. Downloading of copyrighted material for other than personal use;
- d. Using the network for private financial or commercial gain;
- e. Wastefully using resources, such as file space; creating or forwarding chain letters, "spam", or

- other unsolicited or unwanted messages;
- f. Violating End-User Agreements, copyright laws, and fair-use statements from streaming service providers;
 - a. While the District understands the usefulness of streaming media providers such as Netflix, Hulu, and Amazon, these entities explicitly deny the use of their products outside of home use references by the following:
 - 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>
 - b. These resources will not be allowed past the District Firewall unless permission is explicitly granted to use the resource by the provider in writing.
 - g. Creating or sending e-mail or other communications which purport to come from another individual (commonly known as “spoofing”) or otherwise assuming an anonymous or false identity in communicating with other individuals, businesses, or organizations;
 - h. Modifying, disabling, compromising, or otherwise circumventing any anti-virus, user authentication, or other security feature maintained on the District network or any external computer, computer system, or computer account;
 - i. Hacking or gaining unauthorized access to files, resources, or entities;
 - j. Creating or deliberately downloading, uploading, or forwarding any computer virus, or otherwise attempting to modify, destroy, or corrupt computer files maintained by any individual on any computer;
 - k. Compromising the privacy or safety of individuals, which includes the unauthorized disclosure, dissemination, or use of personal identifying information such as personal addresses, telephone numbers, photographs, or other information of a personal nature;
 - l. Using another user’s account or password;
 - m. Disclosing any computer network password (including your own) to any other individual;
 - n. Posting material authored or created by another without his/her consent;
 - o. Posting anonymous messages;
 - p. Using the network for commercial or private advertising;
 - q. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, harassing, or illegal material; and
 - r. Using the network while access privileges are suspended or revoked.
 - s. Engaging in unauthorized use of a personal electronic device to access district network resources.
 - t. Using the computer network to participate in acts constituting “prohibited political activities” under the State Officials and Employees Ethics Act or “election interference” under the Election Code or to participate in any political activities that create an appearance of impropriety under those laws or under any ethics policy of the District relating to political activities of the District’s employees;
 - u. Engaging in any activity that does not meet the intended purposes of the network, as set forth in the Access to Electronic Network Policy and its procedures;
 - v. Communicating with students using non-district controlled technologies, including, but not limited to, social networking sites, without the prior authorization of the Superintendent or his

- or her designee;
- w. Wrongfully and/or inappropriately posting to the web and social media outlets while acting on behalf of the District.
- x. Attempting to commit any action, which would constitute an unacceptable use if accomplished successfully.

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- a. Be polite. Do not become abusive in messages to others.
- b. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
- c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
- d. Recognize that email is not private. People who operate the system have access to all email.
- e. Messages relating to or in support of illegal activities may be reported to the authorities. Do not use the network in any way that would disrupt its use by other users.
- f. Consider all communications and information accessible via the network to be private property (refer to Copyright Web Publishing Rules below).

Non-District Hosted Resources - With the increased usage of free educational applications on the Internet and social media outlets, digital storage areas containing less sensitive User information may or may not be located on the property of the school. In some cases, data will not be stored on local servers. Therefore, Users should not expect that files and communication are private. The District reserves the right to monitor Users' online activities and to access, review, copy and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network and/or Internet access or files, including Google Apps for Education under the District's domain.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - 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 violation the *Access to Electronic Network Policy*, these procedures, or any other rules promulgated by the Superintendent or his or her designee(s).

Security - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Attempts to log on to the Internet 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.

Vandalism - Vandalism will result in the cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other District resource, including District-issued devices. This includes, but is not limited to, the uploading or creation of computer viruses and damage to District devices due to neglect or abuse.

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.

Use of Email – The District provides students, teachers, and staff with Google Workspace for Education, a free web-based program for word processing, spreadsheet, presentation, and web authoring tools. Google Workspace for Education also includes a password-protected email account for school use only.

Google Workspace for Education runs on an Internet domain, which is purchased and owned by the Moline School District and is intended for educational use only. The School District provides email to aid students and staff members in fulfilling their duties and responsibilities and as an education tool.

- a. 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. Unauthorized access by any student or staff member to an email account is strictly prohibited.
- b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
- c. Electronic messages transmitted via the School District's Internet gateway carry with them identification of the user's Internet domain. This domain is a registered 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 the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
- d. 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.
- e. Use of the School District's email system constitutes consent to these regulations.
- f. The school district will NEVER ask you for your password via an e-mail message because we created your account – we can change your password. The best rule of thumb is to never give personal information out through any e-mail you receive requesting personal information.
- g. Reference Document 5:130 AP for the District's backup and retention policy.
- h. Reference Document 6:235AP1-E6 for the Google Workspace for Education policy.

Use of Personal Technology Devices - 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 a personally owned device shall include but are not limited to: streaming media players; iPads, and other tablet PCs; laptop and

netbook computers, cell phones, and smartphones such as iPhone, as well as any device with similar capabilities.

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 burden of responsibility to inquire with school administrators when they are unsure of the permissibility of a particular use of technology before engaging in the use.

District Administration reserves the right to refuse the use of personal technology devices depending upon its 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 responsibility of the User 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.

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 told to stop sending communications, that student must cease the activity immediately.

General Procedure Staff and Students:

- a. The student takes full responsibility for the personal device and keeps it with himself or herself at all times.
- b. The school is not responsible for the security of the personal device.
- c. The user is responsible for the proper care of their personal device, including any costs of repair, replacement, or any modifications needed to use the device at school.
- d. The school reserves the right to inspect a user's personal technology device if there is reason to believe that the user has violated Board policies, administrative procedures, and school rules or has engaged in other misconduct while using their personal device.
- e. Violations of any Board policies, administrative procedures, or school rules involving a student's personally owned device may result in the loss of use of the device in school and/or disciplinary action.
- f. The student must comply with teacher's request to shut down the device or close the screen.
- g. The user may not use the devices to record, transmit or post photos or videos of a person or persons on campus. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of a building administrator.

- h. The user should only use their device to access relevant educational resources related to school.
- i. Staff and students will use the district's secured wireless network. Use of a third-party wireless/cellular connection is not allowed.
- j. Parents/Guardians understand that while the District filters web traffic on personal devices, it DOES NOT track individual student usage or history.
- k. The District assumes that staff and students will abide by the Acceptable Use Agreement (6:235AP1) and all exhibits within that policy.
- l. Refer to document 6:235AP1-E7 for more information.

Internet Safety - Internet access is limited to only those *acceptable uses* as detailed in these procedures. Internet safety is almost assured if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures. Complying with the provisions of the *Access to Electronic Network Policy* and its implementing rules, regulations, and procedures is an important step toward staying safe on the Internet.

Staff members shall supervise students while students are using District Internet access to monitor the student's compliance with the provisions of the *Access to Electronic Network Policy* and its implementing rules, regulations, and procedures.

Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The system administrator and Building Principals shall monitor student Internet access. Despite every effort for supervision and filtering, all users and Students' parents/guardians are advised that access to the network may include the potential for access to content inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and make every effort to avoid those types of content. Every User must report security or network problems to a teacher, administrator, or system administrator.

The District will utilize filtering software or other technologies to prevent Users from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. Attempts to circumvent or 'get around the content filter are strictly prohibited and will be considered a violation of this policy. The District will also monitor the online activities of Users through direct observation and/or other technological means. Not all inappropriate content can be blocked or detected. The District assumes that students, parents/guardians, Administrators, and teachers are aware of inappropriate Internet usage as defined by this policy and will not hold the District accountable for access to inappropriate online material.

Refer to document 6:235AP1-E4 for more information regarding online safety.

Social Media - Social media offers a means by which the District can quickly communicate, share information, and exchange ideas with parents, guardians, staff, and students. Examples of social media use include:

- a. Personal use of social media that references the District, its students, staff, or Board of Education
- b. Classroom use of social media, whether hosted by the District or within the public domain (i.e. Facebook, Twitter, Instagram, YouTube, etc.)
- c. District use of social media s appointed by the Superintendent's office, classroom teacher, or school Administrator.

General Social Media Procedure for Staff and Students

- a. Always comply with any Board of Education policies, procedures, or guidelines.
- b. Use good judgment in all situations.
- c. Assume that all of the information you have shared on your social network is public information.
- d. Be respectful.
- e. Never degrade the District, its students, staff, or Board of Education
- f. Be responsible and ethical.
- g. Never share confidential information about yourself, other students, staff, or Administrators.
- h. Never share personal information.
- i. Understand the terms and conditions of the social media tool being used.
- j. Ensure the integrity of the information being shared.
- k. Report any activity within the social media outlet that is inappropriate, shows abuse, threatens another or depicts harm in any way.
- l. Refer to document 6:235AP1-E10 for more information.

Google Workspace for Education - Google Workspace for Education is a free web-based program that provides educational tools hosted by Google. Google Workspace for Education runs on a domain that is purchased and owned by the District and is intended for educational use only. All students are given a Google Apps for Education account upon acceptance of this Administrative Procedure.

Google Workspace for Education includes the following services:

- a. Mail – an individual email account for school use managed by the District
 - a. Grades K-2 do not have access to email and email addresses are used solely for signing into Workspace Apps.
 - b. Grades 3-4 can only send/receive email to/from specific internal District personnel.
 - c. Grades 5-10 cannot send/receive email from outside the District domain.
 - d. Grades 11-12 can send/receive email to/from any domain.
- b. Calendar – an individual calendar providing the ability to organize schedules, daily activities, and assignments.
 - a. Available for all grade levels.
- c. Drive – a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office
 - a. Available for all grade levels.

- d. Sites – an individual and collaborative website creation tool
 - a. Available for all grade levels.
- e. Classroom – a teacher collaboration tool that allows teachers to post classroom information, retrieve online assignments from students’ Drive and grade materials online.
 - a. Available for all grade levels.

Using these tools, students collaboratively create, edit and share content with teachers, Administrators and other students. These services are entirely online and available 24/7 from many Internet-ready devices. Use of Google Apps for Education implies consent to federal laws, including:

- a. COPPA (Children’s Online Privacy Protection Act). Visit <http://www.ftc.gov/privacy/coppafaqs.shtm> for more information.
- b. Family Educational Rights and Privacy (FERPA). Visit <http://www.ed.gov/policy/gen/guid/fpco/ferpa> for more information.

General Google Workspace for Education Procedure for Students

- a. All students will be assigned a unique Google Workspace for Education account that can be used in accordance with the guidelines listed above per grade level. This account will remain with the student while enrolled in the District.
- b. All guidelines listed in this Administrative Procedure (6:235AP1) and any Board of Education policy apply to the use of Google Workspace for Education.
- c. The school Principal or designee reserves the right to request the revocation of a student’s Google Workspace for Education account if a student is not in compliance with this Administrative Procedure and all District guidelines for acceptable use.
- d. The District does not guarantee the security of electronic files hosted on Google systems.
- e. The District does not guarantee that students will not be exposed to unsolicited information as a result of his/her Google Workspace for Education account.

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

CABINET REVIEWED: October 2016, August 2021, September 2022

ED TECH UPDATED: September 2020, September 2022

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

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

Google Workspace for Education runs on an Internet domain purchased and owned by the Moline-Coal Valley 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-Coal Valley School District's online presence in Google Apps for Education:

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

- Grades K-2 do not have any access to email; accounts are only used to sign in to Workspace apps
- Grades 3-4 can only send/receive email to/from specific teachers and Administrators within the District
- Grades 5-10 cannot send/receive any email from outside the Moline-Coal Valley 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

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. For more information about Moline-Coal Valley School District's Google Workspace for Education program, please visit https://edu.google.com/intl/ALL_us/workspace-for-education/editions/overview/.

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-Coal Valley 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 educational 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>

Guidelines for the responsible use of Google Workspace 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 6:235AP1, and 6:235AP2.
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 to 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.

Google Workspace for Education Permission Form:

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

Under FERPA and corresponding Illinois law, a student's education records are protected from disclosure to third parties.

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 allow my student's education record to be stored 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 the use of Google Workspace for Education (https://edu.google.com/intl/ALL_us/why-google/privacy-security/). I understand that I may ask for my child's account to be removed at any time.

CABINET REVIEWED: December 2017, 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 - 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.

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

- 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