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