Acceptable Use of Electronic Networks and Technology for Students

Instruction

The Moline-Coal Valley Community Unit School District ("District 40 or District") provides technology resources to its students solely for educational purposes. The goal in providing technology resources is to promote educational excellence in District 40 by facilitating resource sharing, innovation, and communication, with support and supervision from parents, teachers, and support staff.

All use of the District's network connection, including Google Workspace and the wide area network (WAN), must support education and/or research and further the Board's stated goals.

Parents or guardians of a District 40 student user must annually acknowledge the District's Acceptable Use Policy during the online registration process for each student in their household. This acknowledgement includes all related administrative procedures and exhibits for the use of District 40's Internet connection. The failure of any user to follow the terms outlined in this administrative procedure will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Board Members, District employees, students, and any District stakeholder using District devices or representing the District in any way must adhere to this policy.

Section 1: Student Guidelines for Google Workspace Accounts

The District provides all students, teachers, and staff with Google Education Workspace accounts, a web-based suite of tools for word processing, spreadsheets, presentations, and web authoring. Google Workspace also includes a password-protected email account for school use only.

Google Workspace runs on an Internet domain purchased and owned by District #40 and is intended for educational use only. This administrative procedure describes the responsibilities of the school, students, and parents in using Google Workspace on the District's domain, in accordance with the District's policies and procedures.

The following services are available to each student and hosted by Google as part of the District's online presence in Google Workspace:

1. **Mail (Gmail) -** an individual email account for school use managed by the Moline School District
    a) Grades K-2 do not have access to Gmail
    b) Grades 3-5 can only send/receive email to/from specific educators within the District
    c) Grades 6-10 cannot send/receive any email from outside the District's domain (only addresses containing @molineschools.org are allowed)
    d) Grades 11-12 are not restricted and can send/receive email to any valid recipient.

2. **Calendar -** an individual calendar providing the ability to organize schedules, daily activities, and assignments
    a) Available for all grade levels
3. **Drive -** a word processing, spreadsheet, drawing, and presentation toolset including cloud-based storage managed by the District's Educational Technology Department.
    a) Available for all grade levels
4. **Sites -** an individual and collaborative website creation tool
    a) Available for all grade levels
5. **Classroom –** A learning management system for course instruction and instructional materials.
    a) Available for all grade levels
6. **Gemini** – an AI-powered platform for enhanced Google searches and research tools.
    a) Not available for students for the 2026-2027 school district.
    b) District 40 reserves the right to enable Gemini for age-appropriate grade levels.
7. **YouTube**
    a) The default status of YouTube for the 2026-2027 school year is ON for all grade levels.

YouTube Management and Restrictions
The District pre-emptively filters YouTube for age-appropriate content using the the District's third-party web filter, the District's firewall, and built-in administrative tools within Google Workspace. Filter controls include:

a) Turning off ads, video suggestions, and comments
b) Implementing YouTube's own strictest content setting
c) Implementing YouTube's settings for age-appropriate material based on grade level
d) Implementing GoGuardian (third-party) filter to filter YouTube videos by grade level

YouTube is a Google service integrated into your child's school Google account, not a separate service. Consent for this procedure (6:235 E:6) includes the managed access your child has to YouTube as defined by the controls above.

8. Additional Core Services

Educational institutions must annually review and reconfirm parental consent to grant students under 18 access to specific Google services. Despite the age requirements a digital tool might list in its Terms of Service, all digital tools used with students must still adhere to all federal and state data privacy laws and all school board policies. Consent for policy 6:235 E:6 includes the managed access your child has to all available Google Workspace Core Services.

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.

Section 2: Board Policy 6:235 - Administrative Procedures

6:235 AP1 (including all associated AP and Exhibits) – Access to Electronic Networks

1. **General Instruction**
    a) All use of District-provided electronic mail (email), the District's network, and the District-provided Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication.
    b) District Network refers to District 40's local area network (LAN - within an individual site), and wide area network (WAN - between sites). This also includes email, shared folders, web servers, telephony systems, intranet, and voicemail.
    c) All information accessed over the World Wide Web (www), websites, email, videos, instant messaging, wikis, blogs, podcasts, and bulletin board systems.
    d) A District Acceptable Use Policy (6:235 and all associated administrative procedures) must be acknowledged during the online registration process before access will be granted to an individual student. At the time of registration, the parent/guardian must annually grant permission for their student.
    e) Guidance and instruction will be provided for each individual granted access through the District. These guidelines do not attempt to state all required or prescribed behavior by users. However, some specific examples are provided.
    f) The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action, as prescribed in Board policy referenced at the end of this agreement.
    g) Acknowledgement of this procedure during the annual online registration process is legally binding and indicates the parent/guardian has read the terms and conditions carefully and understands their significance.

2. **Acceptable Use**. Access to email, the District Network, and District-provided Internet and telephony must be for the purpose of education or research and be consistent with the educational objectives of the District, or for District business.

3. **Privileges.** The use of email, the District Network, and District-provided Internet and telephony is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges.
    a) General rules for behavior and communications apply when using email, the District Network, and the District-provided Internet and telephony.
    b) The administrator, or designee, at each respective site will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time; the decision of the administrator, or designee, is final.
    c) Users will make computers available for inspection by an administrator or designee upon request for the purpose of auditing against this policy.

4. **Unacceptable Use.** The user is responsible for personal actions and activities involving email, social media, websites, the District Network, and District-provided Internet and telephony. Some examples of unacceptable uses are:
    a) Sharing confidential information on students or employees;
    b) Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;

c) Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
d) Using the network for private financial or commercial gain;
e) Wastefully using resources, such as file space;
f) Hacking or gaining unauthorized access to resources or entities;
g) Invading the privacy of individuals;
h) Using another user's account or password;
i) Posting material authorized or created by another without his/her consent;
j) Posting anonymous messages;
k) Using the network for commercial or private advertising;
l) Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, pornographic, threatening, racially offensive, harassing, or illegal material;
m) Using the network while access privileges are suspended or revoked; and
n) Any type of harm to minors or any other person.

5. **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 and social security numbers, of students or colleagues;
    d) Recognize that email is not private:
        1. People who operate the system have access to all emails; and
        2. Messages relating to or in support of illegal activities may be reported to the authorities.
    e) 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 of the district;
    g) Do not use list-serves and distribution lists for distribution of chain mail, jokes or other unprofessional messages; and
    h) Keeping any/all passwords as private, only to be used by appropriate personnel (example: students will not be given the staff password, etc.).

6. **No Warranties.** The District makes no warranties of any kind, whether expressed or implied, for the service it is providing.
    a) 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 users' errors or omissions.
    b) Use of any information obtained via the Internet is at the user's own risk.
    c) The District specifically denies any responsibility for the accuracy or quality of information obtained through Internet services.

7. **Indemnification.** The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District arising out of any violation of these procedures.

8. **Security.**
    a) If the user can identify a security problem accessing the District-provided Internet and District Network (i.e., firewalls and filters), the user must notify the administrator or building principal at the respective site.
    b) Any user must log on to the District network daily in order to ensure updated software downloads, virus protection, and client security.
    c) Demonstration of the problem to other users is prohibited.
    d) Users' accounts and passwords must remain confidential. Revealing your account password to others or allowing others to use your account is prohibited.
    e) Attempts to falsely log on to the Internet or District Network as a system administrator will result in cancellation of user privileges.
    f) Any user identified as a security risk may be denied access to the network.

9. **Vandalism/Harassment.** Vandalism and/or harassment will result in cancellation of privileges and other disciplinary action.
    a) Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, uploading or creating computer viruses.
    b) Harassment is defined as the persistent annoyance of another user or the interference in another user's work. This includes but is not limited to the sending of unsolicited mail.

10. **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.

11. **Social Media and Website Guidelines.**
    a) Any website or social media account used to conduct or communicate about District 40 business must be approved through building and District leadership.
    b) Employees and students must review the Social Media Guidelines on the Intranet and obtain permission from the Public Relations office before creating a social media account.
    c) Due to federal website accessibility laws, all Moline-Coal Valley CUSD 40 employees and students must review the District's web publishing guidelines (6:234 AP2) before publishing any website on behalf of the District.
    d) Freedom of Information laws, student privacy and records laws, and anti-discrimination laws apply to all website and social media accounts.
    e) Copyright law and District policy prohibit the re-publishing of text, graphics, audio, and video without explicit written permission.
        1. This includes the prohibited use of streaming services, such as Netflix, Hulu, Prime Video, and Disney+.
    f) Photos and videos of students can be posted to social media and the web, provided that all students in the photo have parent permission as designated in their student record.
    g) Employees may not post students' last names without receiving special permission in writing from the student's parents/guardians.
    h) The District maintains the right, in its sole discretion, to require students and employees to delete a website or social media account or to remove a specific page, post, tweet, or other content if it violates District 40 policy, procedures, laws, or otherwise is disruptive

to the school or educational environment.

12. **Use of Electronic Mail.** The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an educational 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 electronic mail account is strictly prohibited.
    b) Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.
    c) Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is registered and identifies the author as with the 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 District. Users will be held personally responsible for the content of any and all electronic mail 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) Unauthorized use, or forging, of email header information is prohibited.
    f) Use of the District's electronic mail system constitutes consent to these regulations.

13. District Authorization for Internet Access forms.
    a) Acknowledgement for this procedure for access to electronic networks will be placed in students' temporary files.
    b) Staff forms will be placed in the individual's personnel record and provided by the Human Resources Department.

14. Use of Artificial Intelligence (AI)-Enabled Tools (6:234 AP3).
    a) The Board recognizes that AI-enabled tools are important to enhance student learning, educator effectiveness, and school operations. The use of AI-enabled tools in the District will be implemented safely, ethically, and equitably. To implement the use of AI-enabled tools in the District, the Superintendent or designee will:
        1. Develop a District-wide AI Plan that addresses the District's approach to the integration of AI;
        2. Based on the District-wide AI Plan, establish AI Responsible Use Guidelines to address the responsible use of AI in the District by students and staff;
        3. Ensure that AI-enabled tools comply with State and federal law;
        4. Ensure that staff receive training and students receive instruction on the use of AI, as appropriate; and
        5. Review the District's AI Plan and AI Responsible Use Guidelines on an annual basis and update them as needed.

O. Curriculum.

a) The use of email, the District Network, and the District-provided Internet shall be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students. Such use shall also be consistent with Illinois State Learning Standards.
b) The District will include an annual, age-appropriate curriculum on Internet Safety for students in grades three (3) through eight (8). Recommended topics include:
    1. Safe and responsible use of electronic and internet communication, including cyber-bullying;
    2. Recognizing, avoiding, and reporting online sexual solicitation;
    3. Risks of all electronic transmission of personal information;
    4. Recognition and avoiding unsolicited or deceptive electronic communications;
    5. Reporting of illegal electronic activities and communications; and
    6. Copyright laws on written, photographic, musical, and video materials.

P. Internet Filtering and Monitoring.

a) The District will provide and maintain appropriate Internet filters and monitor the online activities of minors and all users. Such monitoring and filters will include, but not be limited to:
    1. Access by minors to inappropriate Internet materials;
    2. The safety and security of minors and all users using email, Internet chat rooms, and other forms of direct personal communications;
    3. The unauthorized access (including "hacking") and other unlawful online activities by minors and all users;
    4. The unauthorized disclosure, use, or dissemination of personal information regarding minors or other persons;
    5. The restriction of minors' access to harmful materials; and
    6. The unauthorized bypassing of Internet filters and monitoring devices.

Q. Teacher/Student Electronic Communication.

a) The District recognizes that electronic communication may be a useful tool for teacher/student communication about educational matters. In order to assure that all electronic communications between teachers and students are consistent with the goals and policies of the District, District employees may communicate with students only about educational matters and only through:
    1. District electronic accounts and applications such as District email accounts, student information systems like Infinite Campus, and District websites; and
    2. District-approved social networking websites when students are age 13 or older.
    3. Any District employee who wishes to utilize any technology for electronic communication other than those listed above to communicate with students should contact his/her building principal and obtain approval from the Director of

R. Community Relations before utilizing the technology.

a) The District recognized that some employees may maintain personal email accounts, blogs or websites, and/or contribute posts to the blogs or websites or web pages of others, and/or participate in social media. Employees may not communicate with students via these means unless they have a legitimate, independent relationship with the student, such as a familial relationship. Additionally, employees should not follow or friend students or share items they post. Employees who participate in these activities must at all times comply with all legal requirements, including student privacy laws. Employees may not:

1. Disclose student record information, including student work, photographs of students, or any other personally identifiable information about students on their personal sites;
2. Engage in any communication that violates the district's anti-harassment policies;
3. Make or post disparaging, discriminatory, defamatory, confidential, threatening, libelous, obscene, or slanderous comments about the district, its employees, students, or parents (employees are personally liable for their own commentary); or
4. Use district 54 or school logos or email addresses on personal websites or social media accounts.

S. **Website Accessibility.**
District 40 is committed to providing access to its website content for all students, parents, and members of the community, including those with disabilities. The District makes every effort to conform to the Web Content Accessibility Guidelines developed by the World Wide Web Consortium, as well as the Americans with Disabilities Act and Section 504 of the Rehabilitation Act of 1973.

Individuals who want to request an alternate version of any of District 40's web content, ask questions regarding web accessibility or individuals who are unable to access any pages or documents on the District 40 website, can email the community relations department at contact@molineschools.org and indicate the nature of the accessibility or alternative format needs and the URL (web address) of the material.

Section 3: 7:345-AP, E2 – Student Online Personal Protection Act

Student Data Privacy: Notice to Parents About Educational Technology Vendors

School districts throughout the State of Illinois contract with various educational technology vendors for K-12 benefits, such as personalized learning and innovative educational technologies, and increased efficiency in school operations.

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

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

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

a) Basic identifying information, including student or parent/guardian name and student or parent/guardian contact information, username/password, student ID number
b) Demographic information
c) Enrollment information
d) Assessment data, grades, and transcripts
e) Attendance and class schedule
f) Academic/extracurricular activities
g) Special indicators (e.g., disability information, English language learner, free/reduced meals or homeless/foster care status)
h) Conduct/behavioral data
i) Health information
j) Food purchases
k) Transportation information
l) In-application performance data
m) Student-generated work
n) Online communications
o) Application metadata and application use statistics
p) Permanent and temporary school student record information

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

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

Section 4: Related Policy and Federal Law

1. **Children's Online Privacy Protection Act (COPPA)**

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

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

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

2. **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

3. Student Online Privacy Protection Act (SOPPA)

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

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

4. Associated Board Policy (found on the District's website: https://www.boardpolicyonline.com/?b=moline_coal_valley_40):
   a) 6:235 – Access to Electronic Networks
   b) 7:395 – Use of Artificial Intelligence
   c) 7:190/7:190 AP – Student Behavior
   d) 7:210:7:210AP – Student Expulsion from School