Book	Policy Manual
Section	Series 4000 - Instruction
Title	Internet Acceptable Use
Code	4526
Status	Active
Adopted	July 3, 2008
Last Revised	July 24, 2025

INTERNET ACCEPTABLE USE

Purpose and Scope

The Board of Education is committed to optimizing the quality of student learning and faculty teaching. The Board of Education considers student access to computer resources and computer network, as defined below, to be a powerful and valuable educational and research tool and encourages the use of computers and computer-related technology in School District classrooms for the purpose of advancing and promoting learning and teaching. The School District's computer resources and computer network can provide a forum for learning various software applications and through online databases, bulletin boards, and electronic mail, can significantly enhance educational experiences and provide statewide, national, and global communication opportunities for staff and students.

Priority for the use of the School District's computer resources and computer network will be given to those individuals who are using it for curriculum-driven and research-oriented purposes. Official communications from staff and students must be professional, ethical, and meet the standards of other School District publications bearing in mind that the writer is acting as a representative of the School District and in furtherance of the School District's mission.

Definition of Terms

"Authorized users" include members of the Board of Education, administrators, supervisors, faculty, staff, students, parents/persons in parental relation, and any other person who has been granted access to the School District's computer resources.

"Computer resources" include all School District-owned computer hardware, including but not limited to desktop computers, tablets, laptops, calculators and printers; computer software/applications; computer systems and computer networks, including the Internet and wireless networks; telephone equipment; cellular phones/wearables; copy machines; and facsimile machines.

"Computer network" refers to the interconnection of computers, servers, and other electronic devices within a classroom, school, or the School District which facilitates file sharing, resource sharing, communication, collaboration, management, and access to remote resources.

"Personal electronic devices" includes all personally-owned existing and emerging technology devices that can connect to or receive information from the Internet; devices that are able to take photographs; record or play audio or video; input text; upload and download media; or transmit or receive messages, telephone calls or images, including, but not limited to portable storage media; iPod and MP3 players; iPad, Nook, Kindle, and other tablet PCs; Chromebooks, personal laptop and netbook computers; Macbooks; personal digital assistants (PDAs); smart phones such as BlackBerry, iPhone, or Droid; apple watches and other wearables; airpods; or other devices with similar capabilities. The term "personal electronic devices" does not include non-Internet-enabled devices such as cellular phones or other communication devices which are not capable of connecting to the Internet or enabling the user to access content on the Internet.

"School day" is defined as the entirety of the instructional day, during all instructional and non-instructional time, including but not limited to homeroom periods, lunch, recess, study halls, and passing time.

"School grounds" is defined as in or on or within any building structure, athletic playing field, playground, or land contained within the real property boundary lines of the School District's schools.

"Social Media" includes the various online technology platforms and tools that enable people to communicate and share information over the internet including, but not limited to text, audio, video, images, and other multimedia communications.

District Responsibilities

The Superintendent of Schools or his/her designee shall be responsible for designating an individual to act as the computer resources coordinator to oversee the use of School District computer resources and computer network, including preparing in-service programs for the training and development of School District staff and students in connection with the use of same.

The Superintendent of Schools or his/her designee, working in conjunction with the School District's purchasing agent will be responsible for the purchase and distribution of computer software and hardware throughout the School District's schools. They shall prepare and submit for the Board of Education's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or the School District's needs.

Use of the School District's Computer Resources and Computer Network

All School District business being conducted electronically must be performed with a School District account or service. Private email should not be used in connection with School District business. The School District will maintain a list of authorized users which includes, but may not be limited to, students and staff. Users of the School District's computer resources and computer network do so at their own risk.

Whenever an authorized user ceases being a member of the School District community or if such user is assigned a new position and/or responsibilities, use of the School District's computer resources and computer network for which he or she is not authorized in his or her new position or circumstances shall cease and property returned. When a School District employee separates from service from the School District, access to all School District computer resources and computer network, including email, will be disabled.

The use of the School District's computer resources and computer network is a privilege to be used responsibly and appropriately. The same behavioral expectations of staff and students in school apply to the use of personal electronic devices or the School District's computer resources and computer network. Authorized users may download or upload academic/educational files using only platforms authorized by the School District. Removing School District computer resources from the School District's facilities and/or relocating

School District computer resources (not including portable technology devices) requires prior authorization from the Superintendent of Schools or his/her designee.

The School District has installed an Internet filtering system to maintain the integrity of the School District's computer resources and computer network. Notwithstanding the foregoing, the School District cannot guarantee that users will not encounter text, pictures or references that are objectionable when utilizing the School District's computer resources and computer network. Further, even though the School District may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of this Policy.

The School District does not warrant in any manner, express or implied, that the functions or services provided by or through the School District computer resources or computer network will be error-free or without defect. The School District shall not be liable for any liability for any damage suffered by users, including but not limited to, loss of data or interruption of service. Similarly, the School District shall not bear any liability for financial obligations that arise out of the unauthorized, inappropriate, or illegal use of the School District's computer resources or computer network.

No Privacy Guarantee

The School District's computer resources and computer network are the property of the School District. The School District reserves the right to access, view or monitor any information or communication that has been generated or used to access the School District's computer resources and computer network. Electronic data, e.g., may become evidence in legal proceedings. In addition, others may inadvertently view messages or data as a result of routine systems maintenance and monitoring or misdelivery.

Authorized users should not expect, nor does the School District guarantee, privacy associated with their use of the School District's computer resources and computer network. Authorized users should not expect that email, voice mail, or other information created or maintained in connection with the use of the School District's computer resources and computer network (including the use of Google Drive, One Drive or a similar application and even those marked "personal" or "confidential") are private, confidential, or secure. Email used for School District purposes may be subject to disclosure required by law, including pursuant to the Freedom of Information law.

Rules Governing the Use of the School District's Computer Resources and Computer Network

There are risks involved with using the School District's computer resources and computer network. Appropriate behavior is essential in using the School District's computer resources and computer network. Information transmitted using the School District's computer resources and computer network is akin to sending a postcard rather than a sealed letter.

Use of the School District's computer resources and computer network must conform to School District policies and local, state and federal laws. Authorized users should be aware that the School District reserves the right to ensure compliance through electronic monitoring of its computer resources and computer network. Unauthorized use of the School District's computer resources and computer network is strictly prohibited.

In order to maintain the integrity and safety concerning the use of the School District's computer resources and computer network, authorized users:

1. should exercise common sense and discretion when sending or receiving electronic information (e.g., e-mail) utilizing the School District's computer resources or computer network.
2. are responsible for their own accounts and should not share them. Passwords are private and users should not attempt to ascertain the passwords of other users.
3. should never distribute personal information such as addresses, telephone numbers, credit card numbers, social security numbers, bank account numbers, PIN numbers or photographs.
4. should never make appointments to meet people in person whom they have contacted online.
5. should not open email attachments, click on links in emails or download any files from unknown sources.

The following uses of the School District's computer resources are prohibited:

1. Using personal links and addresses such as blogs, YouTube videos, etc. in School District email unless used in the furtherance of business of the School District as part of the curriculum of the School District.
2. Purchasing items or services for personal use.
3. Sharing student user accounts, access private accounts or subscribe to bulletin boards, chat groups or commercial services without the authorization of a designated staff member.
4. Attaching a server to, or providing server services, with the School District's computer resources or computer network (including wireless networks/routers) without authorization from the Superintendent of Schools or designee.
5. Accessing, developing, storing, distributing or promoting illegal activities such as bomb-making, drugs, gambling or pornography.
6. Unauthorized sending of external broadcast email, mass emails, or broadcast voicemail.
7. Promoting discriminatory activities.
8. Installing, using, storing, duplicating or distributing copyrighted materials, including software, games, file, video clips, photographs, graphics, text, music and speech.
9. Plagiarizing the work of others.
10. Promoting political candidates or causes.
11. Commercial advertisements or profit-making purposes.
12. Forging or attempting to forge e-mail messages.
13. Altering electronic communications to hide the identity of the sender.
14. Impersonating another person and/or using the an account owned by another user.
15. Stealing data, equipment or intellectual property.
16. E-mailing files uploading or downloading files which occupy a significant amount of space on the School District's computer resources, or other high volume activities.
17. Changing or exceeding School District computer resource or computer network quotas as set by the School District without the permission of the Superintendent of Schools or his/her designee.
18. Using the School District's computer resources or computer network while access privileges are suspended or revoked.
19. Using the School District's computer resources or computer network in a fashion inconsistent with directions from teachers and other staff and generally accepted etiquette.

20. Failing to maintain the confidentiality of student information in compliance with federal and state law including, but not limited to, FERPA, HIPAA, and Education Law, section 2-d.

21. Accessing the School District's computer resources or computer network to create, access, download, edit, view, store, send or print materials that are illegal, offensive, harassing, intimidating, discriminatory, sexually explicit, or graphic, pornographic, obscene, or which constitute sexting or cyberbullying or are otherwise inconsistent with the values and general standards for community behavior of the School District.

22. Disclosing and/or gossiping (including but not limited to via email, voicemail, Internet instant messaging, social media, chat rooms or on other types of Web pages) about confidential or proprietary information related to the School District.

23. Vandalizing the data of another user.

24. Including external links or graphics that are unrelated to the content of the email.

25. Using the computer resources or computer network for any other unauthorized access including, but not limited to, hacking and/or other illegal activity not specifically enumerated in this policy.

Personal Electronic Device Use by Students

The use of personal electronic devices as defined above by students during the school day anywhere on school grounds is prohibited, unless such use is included in a student's individualized educational plan or 504 plan. Students are not permitted to record classroom instruction unless permitted by the student's individualized educational plan or 504 plan.

Students are required to turn off or silence all personal electronic devices and store them in a school-provided locker at the middle school and high school and in specified classroom storage at the elementary schools upon arrival to school for the entire school day from the opening bell until dismissal in each school building.

The building administration has the discretion to allow students to use personal electronic devices during the school day on school grounds in the following limited instances:

1. if authorized by a teacher, principal, or the School District for a specific educational purpose;

2. where necessary for the management of a student's healthcare;

3. in the event of an emergency;

4. for translation services;

5. on a case-by-case basis, upon review and determination by a school psychologist, school social worker, or school counselor, in conjunction with a school and/or district administrator, for a student caregiver who is routinely responsible for the care and wellbeing of a family member; or

6. where required by law.

Parents/persons in parental relation to students shall be permitted to contact students during the school day by leaving a message with the Main Office of the building where the student attends school. Parents/persons in parental relation to students shall receive written notification of the method(s) and phone number for contacting students upon enrollment and annually at the beginning of each school year.

Further, the School District will not be liable for the loss, damage, theft or misuse of any personal electronic device(s) brought to school. The School District will bear no responsibility nor provide technical support, troubleshooting, or repair of electronic devices owned by anyone other than the School District. Students and staff are responsible for understanding and inquiring about the use of technology prior to engaging in such use.

School District Social Media Platforms

The Board of Education recognizes that social media platforms may be utilized by staff as "content owners" to engage families, community members, students, and employees. The School District's social media platforms provide a mechanism to share information with the school community concerning various events, accolades, and accomplishments in the School District. In addition, social media platforms may be used to provide information regarding school news, closures, or information to be shared with the school community.

School District presence on any social media site, including School District-related accounts, such as clubs, teams, or other sites associated with the School District or a school in the School District must be authorized by the Public Information Officer.

For emergency and data collection purposes only, each School District-related site or social media account must name the Public Information Officer as an administrator. However, the content owner shall be responsible for monitoring and maintaining these accounts. The School District's primary, official social media platforms will be managed by the individual designated by the Superintendent of Schools. Official School District social media accounts will not participate in advertising, nor promote commercial enterprises. School District social media accounts may share relevant community events and updates as approved by the Superintendent of Schools or his/her designee.

Before posting any student work, photographs/videos, or other personally identifiable information (PII), online or to social media, content creators shall review the child's "Release of Information" status to ensure that the parent/person in parental relation has allowed such content to be published digitally. No student photographs or videos should be published for personal, promotional use or any other non-school related purpose. Publishing new pages or modifying existing web pages is permitted only with the written authorization of a designated staff member.

Maintenance and Monitoring Responsibilities

Content owners are responsible for monitoring and maintaining official School District social media accounts as follows:

1. Content must conform to all applicable state and federal laws, as well as the Board of Education's policies and the School District's administrative procedures.

2. Content must not violate any copyright or intellectual property laws and the content owner must secure the consent of all involved parties for the right to distribute materials.

3. Materials taken from the Internet must be properly cited.

4. Confidential information about students, families, staff or School District/Board of Education business and operations (e.g., grades, attendance records, or other pupil/personnel record information) must never be shared.

5. Account administrators must have the profanity filter set to the strongest possible setting on the social media platforms being utilized and hide any inappropriate comments. Postings and comments of an inappropriate nature must be reported and deleted promptly.

6. Postings of a serious nature may warrant additional reporting to the appropriate agency. Such postings include, but are not limited to, threats or inappropriate images.

7. In the event of an emergency/crisis, School District social media platforms shall not be used for providing information or updates concerning the emergency/crisis without the prior written approval of the Superintendent of Schools or his/her designee.

Guidelines for Responsible and Ethical Staff Use of Social Media

1. Work/Personal Distinction - Staff members are encouraged to maintain a clear distinction between their personal social media use and any School District-related social media sites. Personal social media accounts must be kept (other than relatives) separate from work-related accounts.

2. Use of Student Information – Staff members may not send, share, or post pictures, text messages, emails or other material that personally identifies School District students on personal social media pages. Staff members may not use images of students, emails, student examples or work-product, or other personally identifiable student information for personal gain or profit.

3. Professional Conduct – Existing policies and guidelines that cover employee conduct on School District premises and at school-related activities similarly apply to the online environment in those venues.

Consequences of Violations

The School District will respond to complaints of harassing or discriminatory use of the School District's computer resources in accordance with Policy 0100 (Equal Opportunity and Non-Discrimination), Policy 0110 (Sexual Harassment), Policy 0115 (Dignity for All Students Act) and/or Policy 5300 (Code of Conduct). These provisions are not intended to prohibit an authorized user from carrying out his or her assigned educational, employment or administrative function.

The consequences of violating this policy will be consistent with the School District's Code of Conduct and may include the following:

1. Temporary suspension of access to the School District's computer resources and computer network
2. Notification of school authorities
3. Notification of parent/person in parental relation
4. Permanent suspension of access to the School District's computer resources and computer network
5. Financial restitution
6. Disciplinary action
7. Dismissal/termination from the School District
8. Legal action

Any suspected violation of this Policy should be reported immediately to the Superintendent of Schools or designee, as well as to the building principal if the suspected violator is a student.

The Superintendent of Schools or designee shall develop regulations to inform students, teachers and parents/persons in parental relation about the expectations associated with the responsible use of the School District's computer resources and computer network.

Legal	Education Law § 2803
Cross References	0100 - Equal Opportunity and Non-Discrimination 0110 - Sexual Harassment 0115 - Dignity For All Students Act 4526.1 - Internet Safety 5300 - Code of Conduct 8625 - Student, Teacher and Principal Data and Privacy 8630 - Computer Resources and Data Management 8635 - Information Security Breach