PLAINEDGE UNION FREE SCHOOL DISTRICT

ACCEPTABLE USE POLICY **POLICY 4526**

The Board of Education believes that providing access to computers is an integral part of contemporary education. Within financial limitations, computers, computer networks and the internet will be made available to students, faculty and staff. The technology resources at the School District (*e.g.,* all networking, hardware and software, the Internet, e-mail, telephone equipment, digital still and video, voice mail, fax machines and supporting telephone lines, and all communication equipment) are provided to support the educational and administrative activities of the School District and should be used for those purposes. An individual's use of the School District's computer resources must be in support of education and research and consistent with the educational objectives of the School District.

When an individual accesses computers, computer systems and/or computer networks, including the internet (hereinafter the "School District's computer resources") provided by the School District, he/she assumes certain responsibilities and obligations. Access to the School District's computers, computer systems or computer networks is subject to federal, state and local law, as well as Board of Education policy. The use of the School District's computers, computer networks and the internet is a privilege, not a right, and inappropriate use will result in the cancellation of privileges and/or disciplinary action by School District officials.

With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Superintendent of School or designee. The Superintendent of Schools or designee will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements, and if parental permission is needed.

The Superintendent of Schools or designee, working in conjunction with the designated purchasing agent for the School District, will be responsible for the purchase and distribution of computer software and hardware throughout the School District's schools.

Definitions

"Personal electronic devices" and "School District issued devices" include all existing and emerging technology devices that can take photographs; record or play audio or video; input text; upload and download media; connect to or receive information from the internet; and transmit or receive messages, telephone calls or images and include, but are not limited to, personal and School District issued smart devices and electronics including but not limited to: traditional cell phones and flip phones; wearables such as smart watches; iPhones and Android smartphones; Bark phones and other smartphones with modified application menus and parental controls; iPads and other tablets such as Kindles; personal laptops and other computers; air pods and earbuds, all recording devices, and such other Internet connected devices and handheld devices that are available for use.

"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 tools that enable people to communicate and share information over the Internet. Social media can include text, audio, video, images, and other multimedia communications.

"Public social media networks or Social Networking Sites (SNS)" are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the School District community which do not fall within the School District's electronic technology network (*e.g.,* Facebook, MySpace, Twitter, LinkedIn, Flickr, Vine, Instagram, SnapChat, blog sites, etc.).

Administration of the School District's Computer Resources

The individual(s) designated by the Superintendent of Schools, shall:

- oversee the School District's computer resources;
- monitor and examine all network activities, as appropriate, to ensure proper use of the system;
- be responsible for disseminating and interpreting Board of Education and School District policy governing use of the School District's computer resources at the building level with all network users;
- provide employee training for proper use of the School District's computer resources;
- ensure that staff supervising students using the School District's computer resources provide similar training to their students, including providing copies of Board of Education and School District policy governing use of the School District's computer resources;
- ensure that all external drives, disks and software loaded onto the School District's computer resources have been scanned for computer viruses; and
- review staff requests to use 'cloud-based' educational software/applications to ensure that personally identifiable information (PII) is protected in accordance with School District standards prior to student use.

All student agreements to abide by Board of Education policy and parental consent forms shall be signed at the time of registration in the School District. Signed student agreements and parental consent forms shall be kept on file in the School District office.

Internet Access

Students, faculty and staff will be provided with the appropriate Internet access to meet the goals of the School District as stated in this Policy. Student Internet access may be restricted depending on the grade level. In order to access the Internet students must use the School District's network.

There are risks involved with using the Internet. To protect personal safety, Internet users should not give out personal information to others on website, chat rooms or other systems. The School District cannot guarantee that users will not encounter text, pictures or references that are objectionable. Responsible attitudes and appropriate behavior are essential in using this resource. As with e-mail, information that a user places on the Internet is akin to sending a postcard rather than a sealed letter. Its contents may be accessed by system administrators in the School District and elsewhere.

Users must be aware that some material circulating on the Internet is illegally distributed. Users must never use the School District's computer resources to download illegally distributed material. Users are cautioned not to open e-mail attachments or download any files from unknown sources in order to avoid damage to the School District's computer resources. Anything questionable should be reported immediately to the Superintendent of Schools or designee.

With permission, students, faculty and staff may create or modify web pages on the School District web servers which comply in all respects with this policy.

Authorized Use

Authorized users of the School District's computer resources include members of the Board of Education, administrators, supervisors, faculty, staff, students and any other person who has been granted authority by the School District to access its computing, network and telephone systems and whose usage complies with this policy. Unauthorized use is strictly prohibited.

Faculty, staff members and students may be provided with e-mail accounts and Internet access. Staff members may also be provided with e-mail accounts, voice mail accounts, Internet access and other telecommunications upon approval of their supervisors. Whenever a user ceases being a member of the School District community or if such user is assigned a new position or responsibilities, use of the School District's computer resources 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 accounts and email is disabled. All School District business being conducted via email must be performed with a School District account.

The acceptable use of the School District's computer resources will be communicated to all users throughout the School District. Age appropriate instructions regarding acceptable online behavior including interacting with others using the School District technology, cyber bullying awareness and response will be provided by the School District.

Privacy Expectations

The School District's computer resources, including all telephone and data lines, are the property of the School District. The School District reserves the right to access, view or monitor any information or communication stored on or transmitted over the network, or on or over equipment that has been used to access the School District's computer resources. There is no guarantee of privacy associated with an individual's use of the School District's computer resources. Users should not expect that e-mail, voice mail or other information created or maintained in the system (even those marked "personal" or "confidential") are private, confidential or secure.

All users of the School District's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The School District reserves the right to control access to the Internet for all users of its computer resources. The School District may either allow or prohibit certain kinds of online activity, or access to specific websites. Incidental personal use of the School District's computer resources must not interfere with the School District community member's performance, the School District community's ability to use the resources for professional and academic purposes nor violate other School District policies or standards of professional behavior.

Responsible Use

1. All users must act in ways that do not invade the privacy of others and comply with all legal restrictions regarding the use of electronic data.

2. All users must maintain the confidentiality of student information in compliance with federal and state law. Disclosing or gossiping (including but not limited to via e-mail, voice mail, Internet instant messaging, chat rooms or on Web pages) about confidential or proprietary information related to the School District is prohibited.

3. All users must refrain from acts that waste the School District's computer resources or prevent others from using them. Users will not access, modify or delete others' files or system settings without express permission. Tampering of any kind is strictly forbidden. Deliberate attempts to tamper with, circumvent filtering or access, or degrade the performance of the School District's computer resources or telephone system or to deprive authorized users of access to or use of such resources are prohibited.

4. Users are responsible for both the content and possible effects of their messages on the School District's computer resources. Prohibited activity includes, but is not limited to, creating or propagating viruses, material in any form (text, sound, pictures or video) that reflects adversely on the School District, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory, bullying, cyberbullying or harassing material), and billable services.

5. Official email communications 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 educational mission.

6. Users are prohibited from using personal links and addresses such as blogs, YouTube videos, etc. in School District email unless used in the furtherance of the business of the School District or as part of the curriculum of the School District. The signature portion of the user's email may not include external links that are unrelated to the content of the email.

7. Altering electronic communications to hide the identity of the sender or impersonate another person is illegal, considered forgery and is prohibited.

8. Users will abide by all copyright, trademarks, patent and other laws governing intellectual property. No software may be installed, copied or used with or on the School District's computer resources except as permitted by law and approved by the Superintendent of Schools or designee. All software license provisions must be strictly adhered to.

9. Since the installation of applications, other than School District-owned and School District-tested programs could damage the School District's computer resources or interfere with others' use, software downloaded from the Internet or obtained elsewhere must be approved by the Superintendent of Schools or designee. Software may not be installed onto any School District- owned or School District-leased computer by an individual other than the Superintendent of Schools or designee.

10. Use of voice mailboxes for commercial purposes or advertising is not permitted. Use of security codes is required in order to guarantee privacy for mailbox users.

Account Access to Network, E-Mail Accounts and Computer Services

Use of the School District's computer resources shall be governed by the following:

1. All student users of the School District's computer resources will have access according to assigned rights, with appropriate authorization and parent consent in writing. Approved class work shall have priority over other uses. No single user should monopolize a computer, unless specifically assigned for special needs.

2. All use of the School District's computer resources must be in support of education and research or administration/management consistent with the goals of the School District. The term "education" includes use of the system for classroom, professional or career development activities.

3. Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to access their accounts. Users will be held responsible for any policy violations that are traced to their accounts. Under no conditions shall a user provide password to another person.

4. Users will not meet with strangers they have met online.

5. Users may be required to remove files if School District's computer resources storage space becomes low.

6. Users who are provided a School District email address will check their email on a regular basis and delete unwanted messages promptly.

7. Electronic files stored on the school computers may be reviewed by school personnel at any time.

8. The use of group forums, including "chat rooms," for purposes other than education is strictly forbidden.

9. During the school day, students will be allowed Internet access using the School District's computer resources only during instructional time in a controlled environment. A staff member will be required to monitor all of these activities.

System Security

Each user is responsible for the security and integrity of information stored on his or her computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. The School District, at its sole discretion, reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By accessing the School District's system, the individual consents to the School District's right to do so.

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 designee. Unless approved by the Superintendent of Schools or designee, modem use is prohibited on computers that are directly connected to the School District network. Use of personal equipment including, but not limited to printers, scanners, wireless access points (WAP), and switches, is forbidden without special permission from the Superintendent of Schools or designee.

Users may not attempt to circumvent or subvert the security provisions of any other system. Without authorization from the Superintendent of Schools or designee, no one may attach a server to or provide server services on the School District network.

Food and/or drink shall not be placed in the immediate area where computers are located.

Acceptable Use and Conduct

Access to the School District's computer network is provided for educational purposes and research consistent with the School District's mission and goals. Use of the School District's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.

Each individual in whose name an access account is issued is responsible at all times for its proper use. All network users will be issued a login name and password. Passwords must be changed periodically. Users of the network shall only use their assigned passwords and not seek to misrepresent themselves as other users.

All users must 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.

Official email communications 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 educational mission.

All users must adhere to all applicable laws, rules and regulations regarding fair use and copyright.

Only those network users with permission from the principal or individual(s) assigned by the Superintendent of Schools, or who have been issued a School District-owned device, may access the School District's system from off-site (*e.g.,* from home).

All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and swear words are not appropriate.

Network users identifying a security problem on the School District's network must notify the appropriate teacher, administrator, or the Superintendent of Schools or his/her designee. Student users must notify their classroom teacher immediately upon identifying a security problem. Under no circumstance should the user demonstrate the problem to anyone other than to the School District official or employee being notified.

Any network user identified as a security risk or having a history of violations of the School District computer use guidelines may be denied access to the School District's network.

Students and employees are expected to take reasonable precautions to prevent others from using their accounts as they may be held responsible for these actions. Students must immediately notify a staff member if a security problem is identified. Personal contact

information about oneself or other people must not be posted. This includes, but is not limited to, last names, telephone numbers, school or work addresses, and pictures. Email account passwords must not be shared.

Any inappropriate messages received must be immediately reported to a staff member. Students should never meet with someone they have met online without their parent's approval.

Plagiarism and Copyright Infringement

Users will honor all copyright rules and not plagiarize or use copyrighted information without permission. Plagiarism is the use of writings or ideas of others and presenting them as if they were the creation of the presenter.

Any software, music, videos, etc. that are protected under copyright laws will not be loaded onto or transmitted via the network or other on-line servers without the prior written consent of the copyright holder.

The School District will receive written permission from parents and/or guardians prior to publishing any student's work on the Internet or School District web pages. Permission will be obtained in the manner determined by the Superintendent of Schools in their discretion.

Prohibited Activities

The following is a list of examples of prohibited activity concerning use of the School District's computer resources. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the School District's computer resources.

- Knowingly or recklessly posting false or defamatory information about a person or organization.
- Utilizing the School District's computer resources to access, create, download, edit, view, store, send or print material that is illegal, offensive, threatening, 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 is prohibited. For students, a special exception to certain sensitive materials for projects may be made for literature if the purpose of such access is to conduct research and the access is approved by the teacher or administrator. The School District's determination as to whether the nature of the material is considered offensive or objectionable is final. 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), Policy 0110 (Sexual Harassment) and/or Policy 0115 (Student Harassment and Bullying Prevention and Intervention).
- Attempting to log on through another person's account or to access another person's

files, except that the School District's administrators shall have the right to log on through another person's account and access another person's files for network security reasons or other reasons within their discretion.

- Using the School District's computer resources for a purpose or effect that is deemed by the Superintendent of Schools or designee to be dangerous, objectionable, pornographic, distracting to education, or otherwise offensive in nature is prohibited.
- Creating or propagating viruses, material in any form (text, sound, pictures or video) that reflects adversely on the School District, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory, bullying or harassing material), and billable services.
- Cyberbullying and sexting using sexually explicit, graphic, threatening or obscene language or images, or otherwise using language or images inconsistent with the values and general standards for community behavior of the School District.
- Engaging in any illegal act, such as arranging for a drug sale, purchasing alcohol, engaging in criminal activity, threatening the safety of a person, etc.
- Unauthorized exploration of the Network Operating System or unauthorized changes to any installed software.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the School District computer network.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy School District equipment or materials, data of another user of the School District's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Using the network to receive, transmit or make available to others a message that is inconsistent with the School District's Code of Conduct.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the School District's computers and/or network without the permission of the appropriate School District official or employee.
- Using School District's computer resources for commercial purposes or financial gain or fraud. Commercial purposes is defined as offering or providing goods or services or purchasing goods or services for personal use.

- Using the School District's computer resources for political purposes, including political lobbying in support of or opposition to individual candidates or political parties.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Changing or exceeding resource quotas as set by the School District without the permission of the appropriate School District official or employee.
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Invading the privacy of others.
- Failing to comply with all legal restrictions regarding the use of electronic data.
- Disclosing and/or gossiping (including but not limited to via e-mail, voice mail, Internet instant messaging, social media, chat rooms or on other types of Web pages) about confidential or proprietary information related to the School District is prohibited.
- Wasting School District computer resources or preventing others from using them.
- Accessing, modifying or deleting others' files or system settings without express permission. Tampering of any kind is strictly forbidden.
- Deliberately attempting to tamper with, circumvent filtering or access, or degrade the performance of the School District's computer resources or to deprive authorized users of access to or use of such resources.
- Sending broadcast e-mail or broadcast voice mail.
- 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.
- Using School District computers and networks for private or commercial business, advertising, political or religious purposes.
- Student recording of classroom instruction without the express permission of the teacher.
- Attempting to gain unauthorized access to the School District system or to any other computer system through the School District System, or go beyond their authorized access. This includes attempting to access another person's files.
- Deliberately attempting to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means.
- Engaging in illegal acts, such as computer fraud, threatening the safety of self or others, hacking, or engaging in any activity that violates local, state, or federal laws.
- Damaging School District technology in any way.
- Installing software to School District technology, including any downloads, games, hacking tools, music sharing or video sharing applications or others or attempting to run such software from a personal device such as a thumb/flash drive or any other media/device.
- Disclosing passwords to another person.

- Transmitting pictures of themselves or others.
- Attempting to find security problems, as this effort may be construed as an attempt to gain illegal access to the network.
- Attempting to gain unauthorized access to files stored on computers or network servers.
- Using School District technology to post materials or establish email accounts unless required and authorized as part of a curriculum project.
- Making deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or any other means.
- Plagiarizing information found on the Internet.

The School District fully supports the experimental educational and business use of digital resources including, but not limited to, software, third party applications, websites, web-based programs and/or any applications/resources which require a login/password. Since the installation of digital resources, other than School District-owned and School District-tested digital resources, could damage the School District's computer resources, compromise student data/privacy and/or interfere with others' use, digital resources downloaded from the Internet or obtained elsewhere must be approved by the Superintendent of Schools or designee. Digital resources may not be installed onto any School District-owned or School District-leased computer unless in compliance with the Board of Education's policies concerning purchasing and computer resources. Once digital resources have been approved by the Superintendent of Schools or designee, installation will be scheduled and performed.

Social Networking Sites

The School District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach responsible and safe use of these new technologies.

School District Social Media Platforms

The Board of Education recognizes that social media platforms may be utilized by staff as "content owners" to engage parents, 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 Superintendent of Schools or designee. Any accounts existing prior to this policy's adoption will be subject to review.

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 Superintendent of Schools or designee. 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.

Employees have a responsibility for addressing inappropriate behavior or activity on these networks, including compliance with all applicable School District policies. The signature portion of the user's email may not include external links or graphics that are unrelated to the content of the email. Altering electronic communications to hide the identity of the sender or impersonate another person is illegal, considered forgery and is prohibited. Users will abide by all copyright, trademarks, patent and other laws governing intellectual property. No software may be installed, copied or used on School District equipment except as permitted by law and approved by the Superintendent of Schools or designee in accordance with the procedures established for use of software/hardware with the School District's computer resources. All software license provisions must be strictly adhered to.
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 have 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.

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. 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.

4. 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.

5. 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.

6. In the event of an emergency or crisis, School District social media platforms shall not be used for providing information or updates concerning the emergency or crisis without the prior written approval of the Superintendent of Schools or their 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 separate from work-related accounts.

2. Use of Student Information – Staff members shall 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 shall 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 apply to the online environment in those venues.

Student Use of Personal Electronic Devices During the School Day

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 required to turn off or silence all personal electronic devices and store them in a school-provided locker or other location designated by the Building Principal 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:

(i) if authorized by a teacher, principal, or the School District for a specific educational purpose;
(ii) where necessary for the management of a student's healthcare;
(iii) in the event of an emergency;
(iv) for translation services;
(v) on a case-by-case basis, upon review and determination by a school psychologist, school social worker, or school counselor, for a student caregiver who is routinely responsible for the care and wellbeing of a family member; or
(vi) 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 to request a call back from the student. 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.

The School District reserves the right to monitor, inspect, and/or confiscate personal electronic devices when the Building Principal or his/her designee has reasonable suspicion that a violation of this policy has occurred.

Staff Use of Personal Electronic Devices

The Board of Education authorizes staff to use personal electronic device(s) and/or School District issued devices as defined above to access the internet using the School District's computer resources for educational purposes. Individuals connecting to the internet using the School District's computer resources are required to comply with the School District's Internet Safety Policy, as well as the provisions of this policy. Failure to abide by this policy will result in disciplinary action including, but not limited to, revocation of access to the School District's computer resources.

Use of the School District's Computer Resources

The School District maintains a "public" wireless network, a "private" wireless network and a "hard wired" network. The "hard wired" and "private" wireless networks are limited only to district-owned and managed devices. Any attempt to connect a personal electronic device to either of these networks will be considered a violation of this policy. The "public" wireless network is the sole network that students and faculty may connect to using their personal electronic devices. The School District reserves the right to alter or disable access to the "public" wireless network as it deems necessary without prior notification.

Personal electronic devices that have the ability to offer wireless access to other devices must not be used to provide that functionality to others in any School District building. The ability to connect personal electronic devices to the School District wireless network is a privilege and not a right. When personal electronic devices are used in School District facilities or on the School District wireless network, the School District reserves the right to:

1. make determinations on whether specific uses of the personal electronic device is consistent with this policy;

2. log internet use and monitor storage disk space utilized by such users; and

3. remove or restrict the user's access to the internet and suspend the right to use the personal electronic device in School District facilities at any time if it is determined that

the user is engaged in unauthorized activity or in violation of Board of Education policy.

In addition, when staff members choose to use their own personal electronic devices to perform job-related functions, the following will apply:

1. The School District may choose to maintain a list of approved mobile devices and related software applications and utilities. The School District reserves the right to deny any staff member permission to utilize a personal electronic device within the boundaries of the School District. The Superintendent of Schools or designee reserves the right to make these decisions as necessary.

2. Personal electronic devices connected to the internet using the School District's computer resources and/or wireless network must have updated and secure operating systems and proper forms of anti-virus and anti-malware protection. Staff must not make any attempt to connect devices that are not properly secured.

3. The cost to acquire all personal electronic devices is the responsibility of the staff member. Services that include a financial cost to the School District, such as phone options or other "apps" are not allowed. The School District does not agree to pay such charges and staff who desire these options must assume all costs incurred for such charges.

4. Personal electronic devices are not covered by the School District's insurance if lost, stolen or damaged. Loss or damage to any personal electronic device is solely the responsibility of the staff member. If lost or stolen, the loss should be reported immediately to the Superintendent of Schools or designee so that appropriate action can be taken to minimize any possible risk to the School District's computer system and the School District.

5. Staff members shall remain responsible for the maintenance of personal electronic devices, including maintenance to conform to School District standards. Staff members also assume all responsibility for problem resolution, as well as the use and maintenance of functional, up-to-date anti-virus and anti-malware software and any other protections deemed necessary by the Superintendent of Schools or designee.

6. Staff must also meet any expectations of continuity in formatting of files, etc. when making changes to documents for work purposes (*i.e.*, do not change the format of a file so that the original file is unusable on School District-owned hardware/software).

7. All personal electronic devices used with the School District's computer resources is subject to review by the Superintendent of Schools or designee, or individuals/entities designated by the Superintendent of Schools, if there is reason to suspect that the personal electronic device is causing a problem to the School District's computer resources.

8. The use of personal electronic devices in the course of a staff member's professional responsibilities may result in the equipment and/or certain data maintained on it being

subject to review, production and/or disclosure (*i.e.,* in response to a FOIL request, discovery demand or subpoena). Staff members are required to submit any such information or equipment, when requested.

9. Staff members using a mobile device, personal or School District-owned, are responsible for ensuring that all security protocols normally used in the management of School District data on conventional storage infrastructure are also applied on that mobile device. All School District-defined processes for storing, accessing and backing up data must be used on any device used to access the School District's computer system.

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.

Confidentiality and Privacy Rights

Individuals must take all reasonable precautions to prevent unauthorized access to accounts or data by others, both inside and outside the School District. Individuals will not leave any devices unattended with confidential information visible. All devices are required to be locked down when an individual steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Data files and electronic storage areas shall remain School District property, subject to School District control and inspection. The Superintendent of Schools or designee may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy.

Security

1. Each user is responsible for the security and integrity of information stored on his or her computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. The School District, at its sole discretion, reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By utilizing the School District's computer resources, the user has consented to the School District's right to access any and all information thereon.

2. Removing or relocating School District-owned computer resources require prior authorization from the Superintendent of Schools or designee.

3. Users may not attempt to circumvent or subvert the security provisions of any other system. No one may attach a server to or provide server services on the School District

network.

Vandalism

Any act of vandalism is strictly prohibited. Vandalism is the malicious attempt to destroy or harm data or equipment. Uploading, creating or spreading computer viruses is considered to be an act of vandalism. Unauthorized tampering or mechanical alteration, including software configurations is considered to be vandalism.

School District Limitation of Liability

The School District does not warrant in any manner, express or implied, that the functions or the services provided by or through the School District system will be error-free or without defect. The School District will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the user's own negligence or the errors or omissions of any user. Similarly, the School District shall not bear any liability for financial obligations that arise out of the unauthorized or illegal use of the system.

Users of the School District's computer resources, including internet use, do so at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided. 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 the Board of Education and School District policy and regulations.

Users are responsible for any financial costs, liabilities, or damages incurred by the School District as a result of improper use of School District technology, including, but not limited to, equipment (including repairs), replacement of and/or insurance for Chromebooks or other School District issued technological devices, legal fees, and other costs.

Sanctions

All members of the School District community are expected to assist in the enforcement of this policy. Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of computer, telephone or network access privileges, disciplinary action, dismissal or termination from the School District. Some violations may constitute criminal offenses as defined by local, state and federal laws, and the School District may initiate or assist in the prosecution of any such violations to the full extent of the law.

Any suspected violation of this policy should be reported immediately to the Superintendent of Schools or designee. Anyone receiving a threatening message should record/save the message and report the incident to the Principal. The Superintendent of Schools or designee will attempt to trace the message and report the results to the Principal.

The failure to comply with this policy may result in the loss of privileges or access to the School District's computer resources and possible disciplinary action consistent with law, the Code of Conduct or the applicable collective bargaining agreement.

Cross Ref:	Policy 0100	Equal Opportunity
	Policy 0110	Sexual Harassment
	Policy 0115	Student Harassment and Bullying Prevention and Intervention

Ref: Education Law § 2803

Adoption Date: July 1, 2025