VALLEY STREAM UNION FREE SCHOOL DISTRICT TWENTY FOUR

COMPUTER, NETWORK AND INTERNET ACCEPTABLE USE POLICY 6166

The Board of Education believes that providing access to computers is an integral part of a contemporary education. Within financial limitations, computers, computer networks and the internet will be made available to students, faculty and staff. The computer 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, computer software/applications, 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 computer resources is subject to federal, state and local law, as well as Board of Education policy. The use of the School District's computer resources is a privilege, not a right, and inappropriate use will result in the cancellation of privileges and/or disciplinary action by the Superintendent of Schools or his/her designee.

Scope

This policy applies to all authorized users (Board of Education, employees, students and visitors) who access the School District's computer resources using School District-owned or personally-owned equipment, including wireless devices.

When an individual uses or accesses the School District's computer resources provided by the School District, he/she assumes certain responsibilities and obligations. Access to the School District's computer resources is subject to federal, state and local law, as well as Board of Education policy.

Any use of the School District's computer resources that accesses outside resources must conform to the terms and conditions of this policy.

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's computer resources, cyber bullying awareness and response will be provided by the School District.

All information created, stored and/or transmitted on any device or network using the School District's computer resources is subject to the School District's monitoring and review.

All users of the School District's computer resources shall comply with this policy. Failure to comply may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

The Superintendent of Schools shall be responsible for designating an individual(s) to oversee

the use of School District computer resources. Said individual(s) will prepare in-service programs for the training and development of School District staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

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 individual designated by the Superintendent of Schools. This individual 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, working in conjunction with the designated purchasing agent for the School District, the individual(s) assigned to oversee the use of School District computer resources will be responsible for the purchase and distribution of computer resources 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 School District needs.

Purpose

The School District's computer resources 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 and are provided to support the educational and administrative activities of the School District and should be used for those purposes.

All users of the School District's computer resources 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.

1. Use is a privilege, not a right. 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 School District's resources for professional and academic purposes nor violate other School District policies or standards of professional behavior.

2. Use should always be legal, ethical and consistent with the School District's policies on honesty and integrity and its general standards for community behavior.

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

Internet Access

a. 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.
b. Student Internet access may be restricted depending on the grade level.
c. In order to access the Internet students must use the School District's network.
d. All users will be prohibited from: accessing social networking sites; playing online games (unless authorized for School District purposes); purchasing or selling anything online (unless authorized for School District purposes); personal email services; and watching videos online (unless authorized for School District purposes).

A staff member will be required to monitor all internet and network activities as appropriate.

Authorized Use

a. Authorized users include members of the Board of Education, administrators, supervisors, faculty, staff, students, parent/guardian and any other person who has been granted access to the School District's computer resources. Unauthorized use is strictly prohibited. By utilizing the School District's computer resources or personally-owned equipment, the user consents to the School District's exercise of its authority and rights as set forth in this policy with respect to the School District's computer resources, as well as with respect to any information or communication stored or transmitted over the School District's computer resources.
b. Board of Education members, faculty, staff members, and students (where applicable) will be provided with e-mail accounts and Internet access.

c. Whenever a 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 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.
d. All School District business being conducted electronically must be performed with a School District account or service. Employees should not use private email accounts. Email used for School District purposes may be subject to FOIL. There is no expectation of privacy when utilizing School District email.

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

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 this School District and elsewhere. Use of the School District's computer resources shall be governed by the following:

a. All student users of the School District's computer resources will have access according to his/her assigned rights. Approved class work shall have priority over other uses. No single user should monopolize a computer, unless specifically assigned for special needs.
b. 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.
c. 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 his/her password to another person.
d. Users will not meet with strangers they have met on line.
e. Users may be required to remove files if School District's computer resources storage space becomes low.
f. Users who are provided a School District email address will check his/her email on a regular basis and delete unwanted messages promptly.
g. Electronic files stored on the school computers may be reviewed by school personnel at any time.
h. The use of group forums, including "chat rooms," for purposes other than education is strictly forbidden.
i. During the school day, students will be allowed Internet access 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 individual designated by the Superintendent of Schools or his/her designee. Unless approved by the individual designated by the Superintendent of Schools or his/her designee, modem use is prohibited on computers that are directly connected to the School District network. Personal network appliances may not be connected to the School District network and may be confiscated. 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 his/her designee.

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

Users are cautioned not to open e-mail attachments or download any files from unknown sources in order to avoid damaging School District computers and bringing destructive viruses into the School District's system. Anything questionable should be reported immediately to the individual designated by the Superintendent of Schools or his/her designee.

Software shall be installed by the individual designated by the Superintendent of Schools or his/her designee only. The permission of the Superintendent of Schools or his/her designee is necessary in order to download or install software. Permission of the Superintendent of Schools or his/her designee is required for relocation, removal or adjustment of any hardware and/or peripheral device.

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 resources is provided for educational purposes and research consistent with the School District's mission and goals. Use of the School District's computer resources 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 law, rule and regulations regarding fair use and copyright.

Only those network users with written 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 language, sexual language/ images, and/or vulgarities are not appropriate.

Network users identifying a security problem on the School District's network must notify the appropriate teacher, administrator, or the individual designated by the Superintendent of Schools. 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 computer resources.

Students 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. Users must be aware that some material circulating on the Internet is illegally distributed. Users must never use the School District's system to download illegally distributed material.

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.

Prohibited Activities

The following is a list 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 post 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 (Dignity for All Students Act).
- 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 his/her 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 School District's computer resources 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's computer resources.
- 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 computer resources 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 computer resources, uploading, creating or spreading computer viruses and/or unauthorized tampering or mechanical alteration, including software configurations is considered to be vandalism.
- Using the network to send anonymous messages or files.
- Using the computer resources 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 computer resources.
- Installing personal software or using personal disks on the School District's computer resources 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.
- Wastefully using finite School District resources.
- Changing or exceeding resource quotas as set by the School District without the permission of the appropriate School District official or employee.
- Using the School District's computer resources while access privileges are suspended or revoked.
- Using the School District's computer resources 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 the School District's computer resources 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's computer resources or to any other computer system through the School District's computer resources, or go beyond their authorized access. This includes attempting to access another person's files.
- Deliberately attempting to disrupt the School District's computer resources' 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 the School District's computer resources, 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 School District's computer resources.
- Attempting to gain unauthorized access to files stored on the School District's computer resources.
- Using the School District's computer resources 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.

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 individual designated by the Superintendent of Schools or his/her 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 individual designated by the Superintendent of Schools, installation will be scheduled and performed.

1. Altering electronic communications to hide the identity of the sender or impersonate another person is illegal, considered forgery and is prohibited.
2. Users will abide by all copyright, trademarks, patent and other laws governing intellectual property.
3. No software may be installed, copied or used on the School District's computer resources except as permitted by law and approved by the individual designated by the Superintendent of Schools or his/her designee in accordance with the procedures established for use of software/hardware with the School District's computer resources.
4. All software license provisions must be strictly adhered to.

Social Networking Sites

The School District recognizes the importance of teachers, students and parents engaging, collaborating, learning and sharing in digital learning environments as part of a comprehensive approach to 21st century learning. The School District also acknowledges that social media is an integral part of the daily lives of staff, students and the School District community, both in and out of the classroom. While the First Amendment and related laws and court decisions protect a broad spectrum of online speech, they also clearly provide that when one's online posts or other communications disrupt school operations, the conduct may lose its First Amendment protection and subject individuals, including employees, to disciplinary action. Therefore, it is important to create an atmosphere of trust and individual accountability, keeping in mind that online posts and interactions made by the School District's staff and students are a reflection on the entire School District.

Definitions

Online: any virtual or electronic network/space that is accessible by multiple individuals via the internet, intranet or data-based connection

Social Media: forms of electronic communication through which users create or participate in online communities to share information, ideas, personal or group messages and other visual, audio and written content.

Social Media Platforms/Sites: types of online social media communities including but not limited to, Twitter, Facebook, Instragram, SnapChat, VSCO, LinkedIn, Messenger, Pinterest, Yelp, Google, Wordpress, YouTube, blogs, etc.

Cloud-Based Services: virtual data storage and sharing services, including but not limited to, Dropbox, Google Drive, Microsoft OneDrive, Outlook, Gmail, digital photo storage sites, etc.

Guidelines for Social Media Activity

Generally

1. Unless authorized to do so by the Superintendent of Schools or his/her designee, social media posts are not to be identified as official School District communications.
2. Employees are encouraged, and in some cases, required (e.g. pursuant to FERPA), to obtain consent before using or mentioning the names of Board of Education members, employees, students or other members of the School District community on social networking sites.
3. Employees are encouraged to keep their personal social media activities/accounts private from students, so as to maintain the same professional boundaries online as are maintained in the classroom.
4. Unless authorized to do so by the Superintendent of Schools or his/her designee, employees may not use the logos or trademarks associated with individual schools, programs or team of the School District.
5. Employees are individually responsible for their personal posts on social media. Employees may be sued by other employees, parents or others, by any individual that views an employee's social media posts as defamatory, pornographic, proprietary, harassing, libelous or creating a hostile work environment. As these activities are outside the scope of employment, employees are personally liable for related claims.
6. Employees are required to comply with all Board of Education policies and procedures with respect to the use of the School District's computer resources when accessing social media sites.
7. Any access to personal social media activities while on school property, during working hours, or using the School District's computer resources must comply with the School District's policies and may not interfere with an employee's duties at work.
8. If an employee is unsure about the confidential nature of information he/she is considering posting then he/she is strongly encourage to consult with his/her supervisor prior to posting the information.
9. Board of Education members are advised to be cognizant of their simultaneous participation on social media pages/discussions/groups as this may trigger New York State Open Meetings law obligations.
10. Employees and other School District officials must consult with the Superintendent of Schools or his/her designee before deleting posts as certain information may be required to be maintained pursuant to the New York State Records Retention and Disposition Schedule ED-1 or pursuant to other laws, rules regulations.
11. Violation of this policy concerning the use of social media by students, parents of School District community members may lead to legal or disciplinary action consistent with applicable federal and state law.

Prohibited Conduct

The Board of Education does not condone and will take necessary action when social media and online posts and other communications violate the law, Board of Education policies or other

schools rules and regulations including, but not limited to, instances in which online posts/communications:

1. Are harassing, discriminate against others, or otherwise violate New York State or federal law;
2. Are perceived as intimidating or bullying or violate/potentially violate the Dignity for All Students Act ("DASA");
3. Create a hostile environment for staff or students;
4. Contain personally identifiable information about students that is protected by the Family Educational Rights and Privacy Act ("FERPA");
5. Contain information about an individual that is protected from disclosure by the Health Insurance Portability and Accountability Act ("HPAA") or other law;
6. Significantly disrupt School District operations;
7. Contain sexual content;
8. Are libelous/defamatory;
9. Encourage illegal activity;
10. Are threatening or abusive;
11. Contain information that may compromise the health and safety of staff or students; or
12. Contain information or graphics that are subject to a copyright or trademark without first securing prior permission to post the material.

Additional Guidelines for District-Sponsored Social Media Activity

1. Prior to creating a School District sponsored social media account/page, written permission must be obtained from the Superintendent of School or Building Principal, as appropriate. This includes social media accounts/pages created for educational, extracurricular or other School District-related purposes.
2. All user names and passwords for School District sponsored social media accounts/ pages must be provided to the Superintendent of Schools and Building Principal.
3. If an employee wishes to use Facebook, Twitter, Instagram or any other social media site to communicate meetings, activities, games, responsibilities, announcements, etc for an official school-based club, activity, organization, or sports team (hereinafter a "school-based group"), the employee must also comply with the following rules:

    - Access to the site may only be permitted for educational purposes related to the club, activity, organization or team.
    - The account must be a private account, access to which is limited only to participants in the school-based group, including parents of student participants and School District officials.
    - The account must be consistently monitored. Any activity that violates Board of Education policy, including this policy, or other laws, rules or regulations must be immediately reported to the Superintendent of Schools or Building Principal, as appropriate.
    - Access to the account must be approved and regulated by the supervising/monitoring employee. Where possible, the employee will be

responsible for inviting and approving the individuals who are permitted to have access to the group/page.
- When Facebook is used as the social media site, members will not be established as "friends", but as members of the group list. When other social media sites are used, the employee will establish a similar parameter based on the functionality of the social media site utilized.
- Employees are required to maintain appropriate professional boundaries in the establishment and maintenance of the page/group.

4. Employees are required to comply with all Board of Education policies and procedures and all applicable laws, rules and regulations regarding the use of the School District's computer resources when accessing School District sponsored social media sites.
5. Employees may not use School District sponsored social media for private financial gain, political, commercial, advertisement or solicitation purpose.

Use of Personal Electronic Devices/School District Issued Devices

The Board of Education authorizes use of personal electronic device(s) and/or School District issued devices 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 this policy, as well as the provisions of Policy 6167 (Internet Safety). 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.

"Personal electronic devices" or "School District issued devices" include, but are not limited to, personal laptops, smart phones, portable storage media, all recording devices, all Internet connected devices and handheld devices such as Chromebooks, iPods and iPads and include student owned and school district issued devices. With classroom teacher approval, students may use their own devices to access the Internet for educational purposes. The School District reserves the right to monitor, inspect, and/or confiscate personal electronic devices when administration has reasonable suspicion that a violation of school policy has occurred.

The School District maintains a "public" wireless network, a "private" wireless network, an "instructional" wireless network and a "hard wired" network. The "hard wired" and "private" wireless networks are limited only to School 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 employees of the School District 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 employee of the School District permission to utilize a personal electronic device within the boundaries of the School District. The Superintendent of Schools or his/her designee reserves the right to make these decisions in his/her discretion.

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 employee of the School District. 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 employees who desire these options must assume all costs incurred for such charges unless authorized by the Assistant Superintendent for Business.

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 individual designated by the Superintendent of Schools or his/her 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 individual designated by the Superintendent of Schools or his/her 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 are subject to review by the individual designated by the Superintendent of Schools or his/her 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 compliance with 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 resources.

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.

Staff members shall not use their personal electronic devices or cellular phones for personal reasons during the school day except during lunch.

The person to whom the School District has issued an electronic device will be liable for the loss, damage, theft, or misuse of said electronic device(s) issued by the School District. In addition, a student or staff member will be responsible for the full replacement cost of the device if the loaned device is lost, damaged, stolen or misused.

Wireless Policy and Guidelines

Cellular phones, pagers and walkie-talkies are provided to selected members of the School District. Wireless devices including, but not limited to, Chromebooks, iPhones, iPod Touches, iPads and notebook computers are provided to staff members and/or students of the School District. The Assistant Superintendent for Business maintains the inventory for all these devices, auditing of wireless use by the staff, and efficient and effective resolution of billing and service-related issues. The use of wireless technology has been identified by the School District as useful in maintaining communications among the School District community and School District personnel in emergency situations or situations where immediate access to an employee is necessary. The use of such wireless technology is subject to the requirements of the School District's technology and telecommunications practices. By using wireless devices provided by

the School District, the individual consents to the School District's exercise of its authority and rights as set out in this policy.

Cellular Phone Use

Purpose

All School District-issued cellular phones shall be used for the purpose of supporting the School District's education and business objectives. This policy is intended to facilitate effective School District operations relating to cellular phone usage, encourage the responsible use of School District-provided cellular phones, provide guidelines for appropriate cellular phone use, and help manage cellular phone usage costs.

Authorized Users

A list of those employees to whom cellular phones will be given for school business purposes shall be maintained by the Assistant Superintendent for Business and reviewed annually by the Board of Education. This list shall also state with specificity, for each employee, the basis for the issuance of a School District cellular phone.

Acceptable Use Guidelines

1. Cellular phones shall be used only for necessary phone calls in furtherance of school business purposes. Charges or fees for personal cellular phone calls shall be reimbursed by the employee to the School District.
2. The School District shall monitor whether employee cellular phone use or expenses are unreasonable, excessive, personal, unauthorized, or unwarranted.
3. School District cellular phones shall not be used for the purpose of illegal transactions, harassment, obscene or offensive behavior, or other violations of School District policies or law.
4. Cellular phone service contract rights and equipment shall be the property of the School District, and any applicable determinations or changes as to them shall be made by the Business Office.
5. Employees shall have no expectation of privacy in the use of School District cellular phones. All cellular phone bills for School District-issued phones are the property of the School District and will be used as appropriate to investigate the personal use of School District-issued cellular phones.
6. School District cellular phones are valuable and should be handled with due care. If loss, theft, or damage to a School District cellular phone results from the known negligence of the employee to whom such phone is assigned, the employee will be required to reimburse the School District for the repair or purchase of replacement equipment.
7. Upon request, School District-issued cellular phones shall be returned to the appropriate School District official.
8. The School District may discontinue cellular phone privileges at any time.

The Superintendent of Schools or his/her designee shall conduct regular cost-benefit analyses to determine whether the current cellular phone usage is advantageous to the School District, as well as whether cellular phone service plans should be changed in order to reduce costs and maximize the benefit to the School District.

Policy on Wireless Device/Radio Use

The School District insists that all employees act responsibly in their jobs so as not to endanger the lives of themselves or others. No telephone communication, business or personal, is so necessary or urgent that it cannot be postponed or interrupted until such time as the involved person can participate in the phone call without compromising safety. Safe driving is always the first responsibility. The School District actively discourages the use of hand-held cellular phones, and other wireless communication devices, while driving vehicles both on and off School District property, during School District work time or on School District business.

Further, employees should not dial, text, email or otherwise violate the law related to the use of electronic devices while driving on School District business. If an employee must engage in any of the above activities, he or she must pull over to a safe location off the roadway and out of traffic, stop and park the vehicle before doing so. Stopping in a roadway breakdown lane is by its very nature dangerous and therefore is not considered a safe location by the School District.

The School District acknowledges that members of the school administration, members of the facilities department and computer services often use two- way radios and radio-telephones in the School District in the performance of their daily duties. In addition, the use of wireless devices by building administration and security guards are both prevalent and necessary. These employees are reminded to use these devices in such a manner so as not to compromise safety.

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's computer resources will be error- free or without defect. The School District shall not bear any liability for any damage suffered by users including, but not limited to, loss of data or interruption of service. The School District is not responsible for the accuracy or quality of the information obtained through or stored on the School District's computer resources and will not be responsible for financial obligations arising through its unauthorized use. Further, the School District assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided.

Users of the School District's computer resources use information 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 policy.

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 its own negligence or the errors or omissions of any user.

Users are responsible for any financial costs, liabilities, or damages incurred by the School District as a result of improper use of the School District's computer resources, 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.

Confidentiality and 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 and it may be required by law to allow third parties to do so. 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.

Data files and electronic storage areas shall remain School District property, subject to School District control and inspection. The Superintendent of Schools or his/her 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.

Users must recognize that there is no guarantee of privacy associated with their use of School District computer resources. Users should not expect that e-mail, voice mail or other information created with or maintained in the School District's computer resources (including the use of Google Drive or a similar application and even those marked "personal" or "confidential") are private, confidential or secure. If an individual is using his/her personal device to access the School District's network, the individual must keep school work separate from personal files, since school work is subject to School District access. The School District reserves the right to access and view any material stored on the School District's computer resources or any material used in conjunction with the School District's computer resources.

Individuals must also 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.

Policy Enforcement and 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, monetary damages and/or dismissal/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 individual designated by the Superintendent of Schools, as well as to the Principal (if the suspected violator is a student), or the Superintendent of Schools (if the suspected violator is an employee).

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

In the event that a student has violated this policy and/or Code of Conduct as it relates to technology, he/she will be advised of the suspected violation and will be given an opportunity to present an explanation. Violation may result in the suspension of computer privileges and/or other disciplinary action consistent with the School District's Code of Conduct. The School District will fully cooperate with local, state and federal officials in any investigation related to any illegal activities conducted through the School District's computer resources.

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

Cross-ref: 0115 Dignity for All Students Act
5131 Code of Conduct
6165 Computer Resources and Data Management
6167 Internet Safety
6168 Information Security Breach and Notification

Adoption Date: November 21, 1996
Revised: December 19, 2002
Revised: February 15, 2007
Revised: February 24, 2010
Revised: June 18, 2014
Revised: June 12, 2019