(X) Required
( ) Local
( ) Notice

Network and Technology Acceptable Use Policy

The Board of Education recognizes the importance of developing digital literacy and technology competencies, including the ability to use digital tools for communication, expression, collaboration, and access to information. The District believes that curriculum should guide the effective use of technology, not the other way around. Technology should serve as a support for teaching, learning, and administrative practice by improving effectiveness, efficiency, and equity in data management, reporting, communication, and continuous professional and student learning.

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.

Scope

The methods of electronic communication in the Hewlett-Woodmere Public Schools continue to evolve as technology advances. Expectations for the appropriate use of these tools by students and staff remain unchanged. Electronic communications carry the same impact and consequences as any other form of communication and may result in both District-related and legal implications.

It is the responsibility of users to adhere to the District Code of Conduct (Policy #5300) and Code of Ethics (School Board Officer and Employee Ethics Policy # 2160). Since it is ultimately the responsibility of each student's family to set standards and for students to be responsible for their own behavior, we respect each family's right to request restricted access to District network and Internet use by their children where feasible.

Primary access to all District technological resources shall be controlled through provision of individual network user names and passwords. Users must agree to follow established security protocols in place for the protection of network security, data and program integrity, and associated systems and equipment. Users should be aware that all stored information may be accessed by authorized school personnel and that the District reserves the right to ensure compliance through electronic monitoring of ICT networks and Internet usage. Failure to comply with this policy may result in restriction, suspension, or revocation of privileges.

The School District's Network and Technology Acceptable Use Policy applies to all authorized users (Board of Education, employees, students and guests) who access the School District's network or equipment using district-owned or personally owned equipment, including wireless devices.

When an individual uses or accesses the School District's computer hardware (including, but not limited to, desktop computers, tablets, laptops, Chromebooks, printers), computer software/applications, artificial intelligence platforms, computer systems and/or computer networks (including the internet), telephone equipment, cellular phones/watches and/or facsimile machines (hereinafter the "School District's Digital Resources") provided by the School District, he/she assumes certain responsibilities and obligations. Access to the School District's computers, computer systems, and/or computer networks is subject to federal, state, and local law, as well as Board of Education policy.

Purpose

The goal is to provide all users with the tools necessary to meet the educational and administrative objectives of the District, to promote academic excellence, and to develop and hone technological skills.

1. Digital Resources and the Internet are widely available to students and staff in Hewlett-Woodmere Public Schools.

2. The District's technology services offer vast, diverse, and unique resources to users providing access to:
    - Information and Communication Networks: providing shared network resources and applications
    - Internet: providing global information and social networking
    - Email: providing opportunities for electronic interpersonal communication
    - Emerging applications to be adopted as appropriate.

3. The School District's digital resources are provided to support the educational and administrative activities of the School District and should be used for those purposes. Use is a privilege, not a right. Incidental personal use of the School District's digital 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.

4. 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.

5. The District policies, regulations, and handbooks establish rules for behavior and communication applicable to the use of ICT networks and the Internet. The District has established specific rules for the use of the Internet. Students and staff will be trained on the proper use of the Internet. The staff will continue to follow guidelines for appropriate use of instructional material related to the curriculum, but the District cannot guarantee that the users will not have access to improper or unacceptable material. Parents/guardians are advised that communication on the Internet is not censored by the District. By participating in the use of the Internet, students may gain access to information and communication, which they or their parents/guardians may find offensive or inappropriate. Parents/guardians assume this risk by consenting to allow their students to participate in the use of the Internet.

Students may use the Internet only if they have been granted parental permission and have submitted all the required forms.

6. Individuals are responsible for their actions while using the Digital Resources and the Internet. The use of such technology is a privilege, not a right. Inappropriate use may result in restrictions or cancellation of access rights and/or further disciplinary action.

Authorized Use

1. 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 digital resources. Unauthorized use is strictly prohibited. By utilizing the School District's digital 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 digital resources, as well as with respect to any information or communication stored or transmitted over the School District's network.

2. Faculty, staff members, and students (where applicable) may be provided with e-mail accounts and Internet access.

3. The Hewlett-Woodmere Faculty Association has the right to use district email to communicate with its members.

4. 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 digital 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.

5. All School District business being conducted electronically must be performed with a School District account or service. Employees and students 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.

Privacy Expectations

1. The School District's digital 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 network 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.

2. Users must recognize that there is no guarantee of privacy associated with their use of School District digital resources. Users should not expect that email, voice mail or other information created with or maintained in the School District's digital resources (including the use of Google Drive or a similar application and even those marked "personal" or "confidential") are private, confidential or secure.

Responsible Use

1. All users must not act in ways that invade the privacy of others, are unethical or fail to comply with all legal restrictions regarding the use of electronic data. All users must also recognize and not violate the intellectual property rights of others.

2. 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.

3. Users are responsible for the appropriateness and content of material they transmit or publish on the system. Hate mail, harassment, abusive, discriminatory or threatening remarks, bullying, or other antisocial behavior are expressly prohibited. Disclosing and/or discussing (including but not limited to via email, voice mail, Internet instant messaging, social media, artificial intelligence platforms, chat rooms or on other types of Web pages) about confidential or proprietary information related to the School District is prohibited.

4. All users must refrain from acts that waste School District digital 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 digital resources or to deprive authorized users of access to or use of such resources are prohibited.

5. The system is a School District facility and may not be used to support or oppose political candidates or ballot measures. Students may not send broadcast email or broadcast voice mail.

6. Users are responsible for both the content and possible effects of their messages on the network. Prohibited activity includes, but is not limited to, creating or propagating viruses, malware, ransomware, spyware 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.

7. 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.

8. Use of the system to access, store, or distribute obscene, pornographic, or inappropriate material is prohibited.

9. 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 business of the School District as part of the curriculum of the School District.

10. Employees are required to maintain the highest levels of professionalism when communicating through public social media networks or Social Networking Sites (SNS) in their professional capacity as educators. For purposes of this Policy, the definition of 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 District's electronic technology network (e.g., Facebook, YouTube, TikTok, X, LinkedIn, Instagram, Snapchat, etc.).

11. The signature portion of the user's email may not include external links or graphics that are unrelated to the content of the e-mail.

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

13. 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 Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee in accordance with the procedures established for use of software/hardware with the School District's digital resources. All software license provisions must be strictly adhered to.

14. Students are not permitted to record classroom instruction without the express permission of the teacher.

15. 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 and has an Information Technology Staff to support this purpose. Since the installation

of digital resources, other than District-owned and district- tested digital resources could damage the School District's digital 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 Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee. Digital resources may not be installed onto any District-owned or District-leased computer unless in compliance with the Board of Education's policies concerning purchasing and digital resources. Once digital resources have been approved by the Assistant Superintendent for Curriculum, Instruction, and Innovation, installation will be scheduled and performed.

16. Food and beverages may not be brought into computer rooms or consumed while working with District-owned equipment.

17. The Superintendent or designee must approve subscriptions to mailing lists, bulletin boards, chat groups, social networks, commercial on-line services, or other information services. This requirement is waived where access or membership is provided by the District or through District-approved affiliations or professional educational affiliations.

18. The District cannot be held responsible for damages including loss of data resulting from delays or service interruptions. The District is not responsible for the accuracy or quality of information found on the Internet.

Inappropriate Materials

1. The School District prohibits faculty, staff and students from developing, maintaining, and transmitting pornography in any form at school, including, but not limited to, magazines, posters, videos, electronic files or other electronic materials.

2. Accessing the School District's network or equipment to create, access, download, edit, view, store, send or print materials that are illegal, offensive, harassing, intimidating, discriminatory, sexually explicit or graphic, pornographic, obscene, or which constitute sexting or cyberbullying or are otherwise inconsistent with the values and general standards for community behavior of the School District is prohibited. The School District will respond to complaints of harassing or discriminatory use of the School District's digital resources in accordance with Policy 0100 (Equal Opportunity), Policy 0110 (Sexual Harassment) and/or Policy 0115 (Dignity for All Students Act). These provisions are not intended to prohibit an authorized user from carrying out his or her assigned educational, employment or administrative function.

Use of Personal Electronic Devices/School District Issued Devices

The Board of Education only authorizes use of School District issued devices to access the internet using the School District's digital resources for educational purposes. Individuals connecting to the internet using the School District's digital resources are required to comply with the School District's Internet Safety Policy, as well as the provisions of this policy and regulation. Failure to abide by this policy and regulation will result in disciplinary action including, but not limited to, revocation of access to the School District's digital resources.

Students are discouraged from bringing other personal electronic devices to school. If students do bring such devices to school, they must be stored for the entire school day in backpacks or lockers, and they must be silenced and not used during the school day unless permission is granted by an authorized District staff or is part of a students IEP or 504 as required by law (Policy #5695). Any such exception must be formally documented and approved by the District prior to use.

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/guest" wireless network, a "private" wireless network(s), an "instructional" wireless network and a "hard-wired" network. The "hard-wired" and "private" wireless network(s) 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.

Students may not connect any personal electronic devices to any District network without appropriate permission during school hours. 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 (hotspots) 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 his/her designee reserves the right to make these decisions at his/her discretion.

2. Personal electronic devices connected to the Internet using the School District's digital resources and/or wireless network(s) 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. 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 Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee.

5. 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).

6. All personal electronic devices used with the School District's digital resources are subject to review by the Assistant Superintendent for Curriculum, Instruction, and Innovation 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 digital resources.

7. 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.

8. Staff members using a mobile device, personal or 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 system.

Personal electronic devices are not covered by the School District's insurance if lost, stolen or damaged. Further, the School District will not be liable for the loss, damage, theft, or misuse of any personal electronic device(s) brought to school. If lost or stolen, the loss should be reported immediately to the Assistant Superintendent for Curriculum, Instruction, and Innovation 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. 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.

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.

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 Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee may access all such files and communications without prior notice to ensure system integrity and that users are complying with the 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 accessing the District's system, the individual consents to the School District's right to do so.

2. Removing School District digital resources from the School District's facilities and/or relocating School District digital resources (not including portable technology devices) requires prior authorization from the Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee.

3. Unless approved by the Assistant Superintendent for Curriculum, Instruction, and Innovation 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. The use of Virtual Private Networks (VPN's) are not permitted when using District devices or accounts.

4. Storage of copyrighted materials such as music, video and games is prohibited.

5. Users may not attempt to circumvent or subvert the security provisions of any other system. Without authorization from the Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee, no one may attach a server to or provide server services on the School District network.

User Security

Each user will be assigned a *user ID* and *password* for the system.

a. System accounts are to be used only by the authorized user of the account and for authorized purposes. Users may not share their passwords with another person or leave an open file or session unattended or unsupervised. Users are ultimately responsible for all activity under their account if they fail to protect access to their passwords.

b. Users shall not seek information on, obtain copies of, or modify files, other data or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to the system.

c. Individual communications may not be encrypted ~~as~~ to avoid security review except as expressly required to meet state or federal requirements, District financial transactions or as expressly authorized by the Superintendent or designee.

d. Security guidelines will be developed and posted to address the frequency of password changes.

e. Communication and files on the District servers are not private. Network or system administrators may review files and communication to maintain system integrity and ensure that users are using the system responsibly.

f. Password resets in the district will be triggered by security events rather than a predetermined schedule.

g. When assigned District computers or other data access devices, users are required to enable the screen saver lock/password protection option to be set to no more than 15 minutes. Once logged on, users should not leave computers unattended without either logging off or manually enabling the screen saver lock.

h. Users with mobile devices (e.g., smartphones, tablets, laptops, Chromebooks, and other internet-connected devices) providing remote system access, who

elect to store their access codes within the unit, must enable the security lock feature on the device to prevent unauthorized access if the unit is lost or stolen.

i. Passwords are not to be stored or written down in an area where an unauthorized user may gain access. If a user has reason to believe that a password may be compromised, it should be reset immediately.

j. User accounts and passwords for administrative and instructional applications will be administered by the system administrator or designee.

Network Level Security

An administrator or designee shall be responsible for each system or networked software package.

a. All HWPS Technology servers and all vendor hosted servers will be password protected.

b. Permission for access to specific administration rights, for both vendor hosted and HWPS IT servers, programs and operating systems will be approved by the Superintendent or designee.

c. A record of authority approvals and permissions will be maintained in the Office of the Superintendent and a copy will also be on file in the Office of Curriculum, Instruction, and Innovation. The record for the WinCap financial and human resources system will be maintained in the Business Office forwarded quarterly to the Office of the Superintendent.

Personal Security

a. Personal information such as names, addresses, and telephone numbers should remain confidential when communicating on the system. Students should never reveal personal information.

b. Students should never make appointments to meet people in person whom they have contacted on the Internet without District and parent permission.

c. Students should notify their teacher or other adult(s) whenever they encounter information or messages that are dangerous, inappropriate, or make them feel uncomfortable.

d. Social networks have the potential for misuse. Permitted use must be in compliance with all established policies, regulations, and procedures.

The Internet at the School District

1. There are risks involved with using the Internet. To protect personal safety, Internet users should not give out personal information to others on websites,

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 email, 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.

2. Users must be aware that some material circulating on the Internet is copyrighted and subject to all copyright laws. Materials taken from the Internet must be properly cited and credited.

3. 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.

4. Users are cautioned not to open email 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 Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee.

5. With permission, from the appropriate administrator, students, faculty and staff may create or modify web pages on the School District web servers. To ensure the integrity of these sites, users must abide by the School District's web practices. It is the user's responsibility to update and maintain all links and content, keeping in mind the Inappropriate Materials section and the copyright requirements.

WEBSITE POLICY

The Hewlett-Woodmere School District realizes the limitless potential for information and communication provided by the Internet. The availability of this communication vehicle provides an opportunity for students and staff to access and contribute to the world of information related to curriculum, instruction, school, district, and school board related activities. Therefore, the Hewlett-Woodmere School District will use the Internet as an effective, efficient and timely source of information, method of communication and vehicle for resource collection. In order to take advantage of the opportunities the Internet provides, the Board authorizes the creation of school and/or District web pages on the Internet.

Only those web pages maintained in accordance with Board policy and established procedures shall be recognized as official representations of the District or individual schools. All information on a school or district web page must accurately reflect the mission, goals, policies, program, and activities of the school and District. The web page must have a purpose which falls within one of the following categories: 1) Support of

curriculum and instruction-intended to provide links to Internet resources for students, parents, and staff in the District; 2) Public information-intended to communicate information about the schools and District to students, staff, parents, community, and the world at large.

The Superintendent of Schools and/or his designee shall designate an individual(s) to be responsible for maintaining the official district web page and monitoring all district web page activity.

As with any instructional materials or publication used by or representing the school or district, the building principal or district administrator, respectively, is ultimately responsible for accuracy and appropriateness of the information made available on the website. Concern about the content of any page(s) created by students or staff should be directed to the building principal or to the district administrator's office when related to the district web site. If the concern is not resolved, persons wishing to file a formal complaint shall submit a written request for reconsideration of instruction material.

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 shall not bear any liability for any damage suffered by users including, but not limited to, loss of data or interruption of service. Similarly, the School District shall not bear any liability for financial obligations that arise out of the unauthorized or illegal use of the system.

Users of the School District's digital 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.

Policy Enforcement and Sanctions

1. 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.

2. Any suspected violation of this policy should be reported immediately to the Assistant Superintendent for Curriculum, Instruction, and Innovation, as well as to the Principal (if the suspected violator is a student).

Additional Policies and Guidelines for Use of School District Digital Resources

Use of the School District's Digital Resources must comply with the following:

1. Cyber-bullying, sexting, or 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 are prohibited.

2. Anyone leaving such inappropriate messages on voice mail may be subjected to disciplinary action as necessary and appropriate.

3. Anyone receiving a threatening message should record/save the message and report the incident to the Principal. The Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee will attempt to trace the message and report the results to the Principal and Superintendent of Schools.

4. Use of voice mailboxes for commercial purposes or advertising is not permitted.

5. Use of security codes is required in order to guarantee privacy for voicemailbox users.

6. Override permission codes are held by the Principals and the Library/Media Specialists in each school.

7. The unauthorized installation, use, storage, or distribution of copyrighted software or materials on District computers is prohibited.

8. Users are prohibited from plagiarizing work found on the Internet. Plagiarism involves taking the ideas or writings of others and presenting them as if they were your own. This includes but is not limited to generative AI tools (e.g., ChatGPT, Gemini, Copilot)."

Wireless Policy and Guidelines

Smartphones and walkie-talkies may be provided to selected members of the School District custodial, IT, administrative, maintenance and security staff by the Curriculum, Instruction and Innovation department. Wireless devices including, but not limited to, smart phones, mobile hot spots, Chromebooks, Touches, iPads and laptop computers are provided to staff members and/or students of the School District by the Assistant Superintendent for Curriculum, Instruction, and Innovation or his/her designee. The Information Technology Department 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.

Smart Phone Use

Purpose

All District-issued smart phones shall be used solely 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 smart phone usage, encourage the responsible use of District-provided smart phones, provide guidelines for appropriate smart phone use, and help manage smart phone usage costs.

Authorized Users

A list of those employees to whom smart phones will be given for school business purposes shall be maintained by the Assistant Superintendent for Curriculum, Instruction, and Innovation 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 smart phone.

Network and Technology Acceptable Use Guidelines

1. Smart phones shall be used only for necessary phone calls in furtherance of school business purposes. Charges or fees for personal smart phone calls shall be reimbursed by the employee to the School District.
2. The School District shall monitor whether employee smart phone use or expenses are unreasonable, excessive, personal, unauthorized, or unwarranted.
3. School District smart 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. Smart 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 smart phones. All smart phone bills for District-issued phones are the property of the School District and will be used as appropriate to investigate the personal use of district-issued smart phones.
6. School District smart phones are valuable and should be handled with due care. If loss, theft, or damage to a School District-issued smart 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 smart phones shall be returned to the appropriate School District official.
8. The School District may discontinue smart phone privileges at any time.

The Superintendent of Schools or his/her designee shall conduct regular cost- benefit analyses to determine whether the current smart phone usage is advantageous to the School District, as well as whether smart 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 on safety. Safe driving is always the first responsibility. The School District actively discourages the use of hand-held smart phones, and other wireless communication devices, while driving cars, trucks and golf carts both on and off campus, during School District work time or on School District business.

Further, employees should not dial, text, email or otherwise violate state or federal 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 inherently 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 and athletic trainers 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.

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

The Superintendent of Schools or his/her designee will review this policy on a regular basis.

Cross Ref:		
	0100	Equal Opportunity
	0110	Sexual Harassment
	0115	Dignity for All Students Act
	4526.1	Internet Safety
	5300	Code of Conduct
	8630	Digital Resources and Data Management
	8635	Information Security Breach

Adoption Date: August 14, 2017
Amended: February 14, 2018, May 17, 2023, January 21, 2026

Student Account Agreement

Student Section _____

Student Name _____ Grade _____ Date _____

School _____

I have read the District Network and Technology Acceptable Use Policy with my parent/guardian. I agree to follow the rules contained in this Policy. I understand that if I violate the rules my account may be restricted, suspended, or terminated, and I may face other disciplinary measures.

Student Signature_____ Date _____

Parent or Guardian Section

I have read the District Network and Technology Acceptable Use Policy and have reviewed the policy with my child.

I hereby release the District, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my child's use of, or inability to use, the District system, including, but not limited to, claims that may arise from the unauthorized use of the system to purchase products or services.

I will instruct my child regarding any other family restrictions against accessing material beyond those set forth in the District Network and Technology Acceptable Use Policy. I will emphasize to my child the importance of following the rules for personal safety.

I give permission to issue an account for my child and certify that the information contained in this form is correct.

Parent Signature _____Date _____

Parent Name_____

(Please print)

Home Address _____ Phone _____

**********This space reserved for System Administrator**********

Assigned User Name: _____

Assigned Temporary Password:_____

Guest Account Agreement

Name _____

Address _____Phone _____

I have read the District Network and Technology Acceptable Use Policy. I agree to follow the rules contained in this Policy. I understand my account may be terminated as follows:

My account may be terminated at any time upon notice to me. In this event, I will be given the opportunity to remove my personal files.

If my account is unused for more than 30 days, it may be terminated and my personal files removed without notice.

Purpose for which this account is provided:

I agree to limit my use of my account to activities related to the above stated purpose.

I hereby release the District, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my use of, or inability to use, the District system, including, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

Signature _____Date _____

Guest Account authorized by _____

School or Department _____

**********This space reserved for System Administrator**********

Assigned User Name: _____

Assigned Temporary Password: _____

Employee Account Agreement

Name _____

Position _____School or Department _____

I have read the District Network and Technology Acceptable Use Policy. I agree to follow the rules contained in this Policy. I understand that if I violate the rules, I may face disciplinary action in accordance with applicable law.

I hereby release the District, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my use of, or inability to use, the District system, including, but not limited to claims that may arise from the unauthorized use of the system to purchase products or services.

Signature_____ Date _____