Book	Board Policies
Section	7000 PROPERTY
Title	STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	7540.04 AG
Status	Active
Legal	P.L. 106-554, Children's Internet Protection Act of 2000 18 U.S.C. 1460 18 U.S.C. 2246 18 U.S.C. 2256A 20 U.S.C. 6777, 9134 (2003) 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003) 47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
Adopted	March 11, 2024

7540.04 - STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

Staff members shall use District Information & Technology Resources (see definition Bylaw 0100) for educational and professional purposes only.

District Information & Technology Resources (see definition Bylaw 0100) may be used for incidental personal, non-work related purposes that do not interfere with the employee's performance of job responsibilities, do not result in direct costs to the District, do not affect other users use of the resources for education and work-related purposes, do not expose the District to unnecessary risks, or violate applicable Board of Education policies, administrative guidelines, or law/regulations.

Use of District Information & Technology Resources is a privilege, not a right. When using District Technology Resources, staff members must conduct themselves in a responsible, efficient, ethical, and legal manner. Staff members found to have engaged in unauthorized or inappropriate use of District Information & Technology Resources, including any violation of these guidelines, may have their privilege limited or revoked, and may face further disciplinary action consistent with the applicable collective bargaining agreement, Board policy, and/or civil or criminal liability. Prior to accessing or using District Information & Technology Resources, staff members must agree to the Staff Technology Acceptable Use and Safety Policy

This guideline also governs staff members' use of personally-owned communication devices (PCDs) (as defined in Bylaw 0100) when the PCDs are connected to District Information & Technology Resources or when used while the staff member is on Board-owned property or at a Board-sponsored activity. Staff are reminded that use of PCDs (including the sending of text messages) may generate a public or education record that needs to be maintained in accordance with the Board's record retention schedule, litigation hold, and/or Federal and State law.

Below is a non-exhaustive list of unauthorized uses and prohibited behaviors. This guideline further provides a general overview of the responsibilities users assume when using District Information & Technology Resources.

A. All use of District Information & Technology Resources must be consistent with the educational mission and goals of the District.

B. Staff members may only access and use District Information & Technology Resources by using their assigned account and may only send school-related electronic communications using their District-assigned e-mail addresses or services/apps connected/linked to their District-assigned e-mail addresses. Use of another person's account/e-mail address is prohibited. Staff members may not allow other users to utilize their account/e-mail address and should not share their password or other multifactor authentication (MFA) device/app with other users. Staff members may not go beyond their authorized access. Staff members are expected to take steps to prevent unauthorized access to their accounts by logging off or "locking" their PCDs when leaving them unattended and employing MFA techniques whenever possible/available.

C. No user may access another person's private files. Any attempt by users to access another user's or the District's non-public files, or phone or e-mail messages, is prohibited. Any attempts to gain access to unauthorized resources or data/information located on District Information & Technology Resources are prohibited. Similarly, staff members may not intentionally seek data/information on, obtain copies of, or modify files, data, or passwords belonging to other users, or misrepresent other users on District Information & Technology Resources.

D. Staff members may not intentionally disable any security features used on District Information & Technology Resources.

E. Staff members may not use District Information & Technology Resources or their PCDs to engage in vandalism, "hacking" or other illegal activities (e.g., software pirating; intellectual property violations; engaging in slander, libel, or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; and/or sale of illegal substances or goods).

   1. Slander and Libel - In short, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting, or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Staff members shall not knowingly or recklessly post/publish false or defamatory information about a person or organization. Staff members are reminded that material distributed over the Internet is "public" to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people, and harmful and false statements will be viewed in that light.

   2. Staff members shall not use District Information & Technology Resources to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex (including sexual orientation or gender identity), age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, text messages, e-mails, or other materials of a sexual nature (e.g., sexting) in electronic or any other form, including the contents of a PCD or other electronic equipment is grounds for discipline, up to and including termination. Such actions will be reported to local law enforcement and child services as required by law.

   3. Vandalism and Hacking – Deliberate attempts to damage the hardware, software, or data/information residing in District Information & Technology Resources or any computer system attached through the Internet is strictly prohibited. In particular, malicious use of District Information & Technology Resources to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system is prohibited.

      Attempts to violate the integrity of private accounts, files, programs, or services/apps, the deliberate infecting of District Information & Technology Resources or PCDs attached to the network with a "virus", and/or attempts at hacking into any internal or external computer systems using any method will not be tolerated.

      Staff members may not engage in vandalism or use District Information & Technology Resources or their PCDs in such a way that would disrupt others' use of District Information & Technology Resources.

      Vandalism is defined as any malicious or intentional attempt to harm, steal, or destroy data/information of another user or District Information & Technology Resources.. This includes, but is not limited to, creating and/or uploading of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network security and/or the Board's Information & Technology Resources protection measures. Staff members also must avoid intentionally wasting limited resources. Staff members must immediately notify theBuilding

Administrator if they identify a possible security problem. Staff members should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

4. Use of District Information & Technology Resources to access, process, distribute, display, or print child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and material that lacks serious literary, artistic, political, or scientific value as to minors. If a staff member inadvertently accesses material that is prohibited by this paragraph, the staff member should immediately disclose the inadvertent access to theBuilding Administrator. This will protect the staff member against an allegation that the staff member intentionally violated this provision.

5. Unauthorized Use of Software or Other Intellectual Property from Any Source – Laws and ethics require proper handling of intellectual property. Software is intellectual property and, with the exception of freeware, is illegal to use without a legitimate license or permission from the software's creator or licensor. All software loaded on District Information & Technology Resources must be approved by the District Technology Staff, and the District must own or otherwise obtain, maintain, and retain the licenses for all copyrighted software loaded on District Information & Technology Resources. Staff members are prohibited from using District Information & Technology Resources for the purpose of illegally copying another person's software. Illegal peer-to-peer file trafficking of copyrighted works is prohibited.

   Online articles, blog posts, podcasts, videos, and wiki entries are also intellectual property. Staff members should treat information found electronically in the same way they treat information found in printed sources – i.e., properly citing sources of information and refraining from plagiarism.

F. Transmission of any material in violation of any State or Federal law or regulation, or Board policy, is prohibited.

G. Staff members may not use District Information & Technology Resources for private gain or commercial purposes (e.g., purchasing or offering for sale personal products or services by staff members), advertising, or political lobbying or campaigning.

H. Staff members are expected to abide by the following generally accepted rules of online etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through or utilizing District Information & Technology Resources. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive, or disrespectful language in communications made through or utilizing District Information & Technology Resources (including, but not limited to, public messages, private messages, and material posted on web pages).

2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.

3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a staff member is told by a person to stop sending them messages, the staff member must stop.

4. Do not post information that, if acted upon, could cause damage or a danger of disruption.
5. Regularly check District-provided e-mail account and delete e-mails no longer need. Nothing herein alters the staff member's responsibility to preserve e-mail and other electronically stored information that constitutes a public record, a student education record, and/or a record subject to a Litigation Hold.

I. All communications and information accessible via the Internet should be assumed to be private property (i.e., copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions/acknowledgment of authorship must be respected.

J. Downloading of information onto school-owned equipment or contracted online educational services is prohibited without prior approval from the District Technology Staff. If a staff member transfers files from information services, the staff member must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a staff member transfers a file or installs a software program that infects District Information & Technology Resources with a virus and causes damage, the staff member will be liable for any and all repair costs to make District Information & Technology Resources once again fully operational.

K. Privacy in communication over the Internet and through the District's Information & Technology Resources is not guaranteed. In order to verify compliance with these guidelines, the Board reserves the right to access, monitor, review, and inspect any directories, files, and/or messages stored on or sent/received using District Information & Technology Resources. Messages relating to or in support of illegal activities will be reported to the appropriate authorities

   The following Notice will be included as part of the computer log-on screen:

   "District Information & Technology Resources (as defined in Bylaw 0100) are to be used for educational and professional purposes only. Users are reminded that all use of District Information & Technology Resources, including Internet use, is monitored by the District and individual users have no expectation of privacy."

L. Use of the Internet and any data/information procured from the Internet is at the staff member's own risk. The Board makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through District Information & Technology Resources will be error-free or without defect. The Board is not responsible for any damage a user may suffer including, but not limited to, loss of data, service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of information obtained through the Internet. Information (including text, graphics, audio, video, etc.) from Internet sources used in class must be cited the same as references to printed materials. The Board is not responsible for financial obligations arising through the unauthorized use of District Information & Technology Resources. Staff members will indemnify and hold the Board harmless from any losses sustained as the result of the staff member's misuse of District Information & Technology Resources.

M. Disclosure, use, and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Technology Acceptable Use and Safety Agreement Form".

N. Proprietary rights in the design of websites, web pages, and services/apps hosted on Board-owned or District-affiliated servers remain at all times with the Board without prior written authorization.

O. Staff members are reminded that student personally identifiable information is confidential and may not be disclosed without prior written permission from a student (eighteen (18) years of age or older) or the parent/guardian of a minor student (seventeen (17) years of age or younger).

P. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the District's users will be fully investigated and disciplinary action will be imposed as appropriate.

Q. Preservation of Resources: District Information & Technology Resources are limited. Each staff member is permitted reasonable space to store e-mail, web, and personal school/work related files. The Board reserves the right to require the purging of files in order to regain space on the data storage devices.

R. Staff members are required to limit student exposure to commercial advertising and product promotion when selecting/developing the District or classroom websites, web pages, or services/apps or giving other assignments that utilize the Internet. Under all circumstances, staff members must comply with COPPA.

   1. Websites with extensive commercial advertising may be included on the District or classroom websites, web pages, and/or services/apps or designated as a required or recommended site only if there is a compelling educational reason for such selection.

   2. Staff members may make use of high-quality, unbiased online educational materials that have been produced with corporate sponsorship. Staff members may not make use of educational materials that have been developed primarily for the purpose of promoting a company and/or its products or services.

S. Artificial Intelligence/Natural Language Processing Tools: Staff are permitted to use Artificial Intelligence and Natural Language Processing (NLP) tools (collectively, “AI/NLP tools”) to accomplish their job responsibilities, so long as the use is ethical, responsible, and does not violate any provisions of this guideline – e.g., it does not infringe on students’ or staff members’ privacy rights, violate their duty to maintain confidentiality related to personally identifiable information, etc.). With respect to students, absent express direction/permission from a teacher, a student may not use AI/NLP tools to complete school work – i.e., to create, compose, generate, or edit original content that they intend to submit as their own work. This prohibition includes, but is not limited to, the use of AI/NLP tools to prepare a writing assignment or creative art project, or to answer questions on a quiz, test, or in-class or homework assignment. The preceding prohibition does not include and does not limit a student’s use of AI/NLP tools that are features built into apps, including a word processing program, installed by the District on

District-issued PCDs (e.g., Chromebooks), or AI/NLP tools that is/are listed as approved accommodation(s) or assistive technology pursuant to a student's individualized education program or Section 504 Plan. In particular, this prohibition does not include the use of speech-to-text features that are part of District-issued PCDs unless the purpose of the class work/assignment is to assess/test a student's knowledge of spelling, grammar, etc. If a student has any question as to whether specific AI/NLP tools can be used for an assignment, the student is expected to ask their teacher. If a student violates this prohibition, the student will be charged with plagiarism and disciplined in accordance with the Student Code of Conduct, including not receiving credit for the assignment.

Abuse of Network Resources

Peer-to-peer file sharing, unsolicited/external mass mailings, and downloading of unauthorized games, videos, and music are wasteful of limited network resources and are forbidden. In addition, the unauthorized acquisition and sharing of copyrighted materials are illegal and unethical.

Unauthorized Printing

District printers may only be used to print school/work-related documents. Printers, like other school resources, are to be used in a responsible manner. Ink cartridges and paper, along with printer repairs and replacement, are very expensive. The District monitors printing by a user. Print jobs deemed excessive and abusive of this privilege may result in charges being assessed to the staff member.

Any questions and concerns regarding these guidelines may be directed to the Superintendent/designee.