Book	Board Policies
Section	7000 PROPERTY
Title	STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	7540.03 AG
Status	Active
Legal	P.L. 106-554, Children's Internet Protection Act of 2000 20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003) 18 U.S.C. 1460 18 U.S.C. 2246 18 U.S.C. 2256 20 U.S.C. 6777, 9134 (2003) 47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
Adopted	March 11, 2024

7540.03 - STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY

Students shall use District Information & Technology Resources (see definition Bylaw 0100) for educational purposes only. District Information & Technology Resources shall not be used for personal, non-school related purposes. Use of District Information & Technology Resources is a privilege, not a right. When using District Information & Technology Resources, students must conduct themselves in a responsible, efficient, ethical, and legal manner. Students who engage 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 Student Code of Conduct/Student Handbook and/or civil or criminal liability. Prior to accessing or using District Information & Technology Resources, students (eighteen (18) years of age and older) and parents of minor students must acknowledge that they have read the Student Acceptable Use Policy Parents should discuss their values with their children and encourage students to make decisions regarding their use of District Information & Technology Resources that are in accord with their personal and family values, in addition to the Board's standards.

This guideline also governs students' use of personally-owned communication devices (PCDs) (see definition Bylaw 0100) when the PCDs are connected to District Information & Technology Resources or when used while the student is on Board-owned property or at a Board-sponsored activity.

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. Students 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 email addresses. Use of another person's account/e-mail

address is prohibited. Students 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. Students may not go beyond their authorized access. Students should take steps to prevent unauthorized access to their accounts by logging off or "locking" their District Information & Technology Resource/Device(s)/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 on District Information & Technology Resources or other services/apps are prohibited. Similarly, students may not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, or misrepresent other users on the District's Information & Technology Resources.

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

E. Students 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; or sale of illegal substances and 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.) Students shall not knowingly or recklessly post/publish false or defamatory information about a person or organization. Students 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. Students 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. 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 information residing in District Information & Technology Resources or any services/apps attached through the Internet are strictly prohibited. In particular, malicious use of District Information & Technology Resources to develop programs that harass other users or infiltrate District Information & Technology Resources or PCDs and/or damage District Information & Technology Resources or PCDs 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.

   Students 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 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 technology protection measures. Students also must avoid intentionally wasting limited resources. Students must immediately notify a teacher or Principal, if they identify a possible security problem. Students 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 student inadvertently accesses material that is prohibited by this paragraph, the student should immediately disclose the inadvertent access to a teacher or Principal. This will protect the user against an allegation that the user intentionally violated this provision.

5. Unauthorized Use of Software or Other Intellectual Property from Any Source – All communications and information accessible via the Internet should be assumed to be private property (i.e., copyrighted and/or trademarked). Laws and ethics require proper handling of intellectual property. All copyright issues regarding software, information, and attributions/acknowledgment of authorship must be respected.

   Software is intellectual property and, with the exception of freeware, is illegal to use without legitimate license or permission from its creator or licensor. All software loaded on District Information & Technology Resources must be approved by the Director, and the District must own or otherwise obtain, maintain, and retain the licenses for all copyrighted software loaded on District computers. Students 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. Students 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. Rules against plagiarism will be enforced.

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

G. Students 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 students), advertising, or political lobbying.

H. Students may not use District Information & Technology Resources to engage in cyberbullying. "Cyberbullying" involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, which is intended to harm others. Cyberbullying may occur through e-mail, instant messaging (IM), chat room/Bash Boards, small text messages (SMS), websites, voting booths,social media, and other technological means of communicating/publishing text, audios, and/or videos.

   Cyberbullying includes, but is not limited to, the following:

   1. posting/publishing slurs or rumors or other disparaging remarks about a student on a website or weblog;

   2. sending e-mails or instant messages that are mean or threatening or so numerous as to negatively impact the victim's use of that method of communication and/or drive up the victim's cell phone bill;

   3. using a smartphone to take and/or send embarrassing and/or sexually explicit photographs/recordings of students;

   4. posting/publishing online misleading or fake photographs of students.

I. Students 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.

   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 student is told by a person to stop sending that person messages, the student must stop.

   4. Do not post information that, if acted upon, could cause damage or a danger of disruption.

5. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet. This prohibition includes, but is not limited to, disclosing personally identifiable information on commercial websites.

6. Do not transmit to third parties/unknown individuals pictures or other information that could be used to establish identity without prior approval of a teacher.

7. Never agree to get together with someone you "meet" online without parent approval and participation.

8. Regularly check District-provided e-mail account and delete e-mails no longer need.

9. Students should promptly disclose to a teacher/building administratorany messages they receive that are inappropriate or make them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). To aid in any investigation, students should not delete such messages until instructed to do so by an administrator.

J. Downloading of files onto District Information & Technology Resources is prohibited without prior approval from the District. If a student transfers files from online services/apps the student must check the file with a virus detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or installs a program that infects District Information & Technology Resources with a virus and causes damage, the student will be liable for any and all repair costs associated with making the District Information & Technology Resources once again fully operational.

K. Students must secure prior approval from a teacher or the building administrator before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or Listservs.

L. Students are prohibited from accessing or participating in online "chat rooms" or other forms of direct electronic communication (e.g., instant messaging) (other than e-mail) without prior approval from a teacher or the building administrator. All such authorized communications must comply with these guidelines. Students may only use their school-assigned accounts/e-mail addresses when accessing, using, or participating in real-time electronic communications for education purposes.

M. 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 residing on or sent using the District's Information & Technology Resources. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

N. Use of the Internet and any data/information procured from the Internet is at the student's own risk. The Board makes no warranties of any kind, either express or implied, that the functions or 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/information, service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of data/information obtained through the Internet. Data/Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects must be cited the same as references to printed materials. The Board is not to be responsible for financial obligations arising through the unauthorized use of District Information & Technology Resources. Students or parents of students will indemnify and hold the Board harmless from any losses sustained as the result of a student's misuse of District Information & Technology Resources.

O. 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 Acceptable Use Policy".

P. 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.

Q. 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.

R. Preservation of Resources and Priorities of Use: District Information & Technology Resources are limited. Each student is permitted reasonable space to store e-mail, web, and personal school-related files. The Board reserves the right to require the purging of files in order to regain space on data storage devices. Students who require access to District Technology Resources for class- or instruction-related activities have priority over other users.

Students not using District Information & Technology Resources for class-related activities may be "bumped" by any student requiring access for a class- or instruction-related purpose.

Game playing is not permitted unless under the supervision of a teacher/building administrator.

U. Artificial Intelligence/Natural Language Processing Tools: Absent express direction/permission from a teacher, a student may not use Artificial Intelligence (AI) or Natural Language Processing (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 and 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(s) as to whether specific AI/NLP tools can be used for an assignment, the student should 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, mass mailings, and downloading of unauthorized games, videos, and music are wasteful of limited network resources and 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-related documents and assignments. 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 users. Print jobs deemed excessive and abusive of this privilege may result in charges being assessed to the student. Users are prohibited from replacing ink cartridges and performing any other service or repairs to printers. Users should ask, as appropriate, for assistance to clear paper that is jamming a printer.

Any questions and concerns regarding these guidelines may be directed to the Teacher/Building Administrator.