Farland Local School District Acceptable Use and Safety Policy 2026-2027

TECHNOLOGY

The Board of Education is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of District operations.

Students' use of District Information & Technology Resources (see definitions in Bylaw 0100) is a privilege, not a right. Students and their parents must sign and submit a *Student Technology Acceptable Use and Safety* form annually. (See also, Policy 7540.03)

The DTP shall set forth procedures for the proper acquisition of technology. The DTP shall also provide guidance to staff and students about making safe, secure, appropriate, and ethical use of District Information & Technology Resources, as well as inform both staff and students about disciplinary actions that will be taken if its Information & Technology Resources are abused in any way or used in an inappropriate, illegal, or unethical manner. See Policy 7540.03 and AG 7540.03 - Student Technology Acceptable Use and Safety, and Policy 7540.04 and AG 7540.04 – Staff Technology Acceptable Use and Safety.

This policy, along with the Student and Staff Technology Acceptable Use and Safety policies and the Student Code of Conduct, further govern students' and staff members' use of their personal communication devices (see Policy 5136 and Policy 7530.02). Users have no right or expectation of privacy when using District Information & Technology Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using District Information & Technology Resources).

Further safeguards shall be established so that the Board's expenditure of public funds to acquire, operate, and maintain District Information & Technology Resources achieves the desired benefits and inhibits negative side effects. Accordingly, students shall be educated about appropriate online behavior including, but not limited to, using social media, which is defined in Bylaw 0100, to interact with others online; communicating with other individuals in chat rooms or using other messenger apps, or through blogs, audios (e.g., podcasts), and videos; and recognizing what constitutes cyberbullying, understanding cyberbullying is a violation of Board policy, and learning appropriate responses if they experience cyberbullying.

Staff use of District-approved social media platforms/sites shall be consistent with Policy 7544.

Students must comply with Policy 5136, Policy 5722, Policy 7540.03, and Policy 7544 when using District Information & Technology Resources to access and/or use District-approved social media.

Similarly, staff must comply with Policy 7544, Policy 7540.04, and Policy 7530.02 when using District Information & Technology Resources to access and/or use District-approved social media platforms/sites.

STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY

Technology directly affects the ways in which information is accessed, communicated, and transferred in society. Educators are expected to continually adapt their means and methods of instruction and the way they approach student learning to incorporate the latest technologies. The Board of Education provides Information & Technology Resources (as defined in Bylaw 0100) (collectively, "District Information & Technology Resources") to support the educational and professional needs of its students and staff. With respect to students, District Information & Technology Resources afford them the opportunity to acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board provides students with access to the Internet for educational purposes only and utilizes apps and services (as defined by Bylaw 0100) to enhance the instruction delivered to its students. The District's computer network and Internet system do not serve as a public access service or a public forum and the Board imposes reasonable restrictions on its use consistent with its stated educational purpose.

The Board regulates the use of District Information & Technology Resources in a manner consistent with applicable local, State, and Federal laws, the District's educational mission, and articulated expectations of student conduct as delineated in the Student Code of Conduct. This policy and its related administrative guidelines and the Student Code of Conduct govern

students' use of District Information & Technology Resources and students' personal communication devices ("PCDS") when they are connected to District Information & Technology Resources, including apps/services, regardless of whether such use takes place on or off school property (see Policy 5136).

Students are prohibited from using District Information & Technology Resources to engage in illegal conduct (e.g., libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, etc.) or conduct that violates this Policy and its related administrative guidelines and the Student Code of Conduct (e.g., making personal attacks or injurious comments, invading a person's privacy, etc.). Nothing herein, however, shall infringe on students' First Amendment rights. Because its Information & Technology Resources are not unlimited, the Board may institute restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.
Students have no right or expectation to privacy when using District Information & Technology Resources (including, but not limited to, privacy in the content of their personal files, messages/e-mails, and records of their online activity).

While the Board uses various technologies to limit students using its Information & Technology Resources to only use/access apps/services and other resources that have been pre-approved for the purpose of instruction, study, and research related to the curriculum, it is impossible to prevent students from accessing and/or coming in contact with online content that has not been pre-approved for use by students of certain ages. It is no longer possible for educators and community members to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them) when significant portions of students' education take place online or through the use of apps/services.

Pursuant to Federal law, the Board implements technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act (CIPA). At the discretion of the Board or the Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor the online activity of students to restrict access to child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using District Information & Technology Resources if such disabling will cease to protect against access to materials that are prohibited under CIPA. Any student who attempts to disable the technology protection measures will be disciplined.

The Superintendent may temporarily or permanently unblock access to websites or apps/services containing appropriate material if access to such sites has been mistakenly, improperly, or inadvertently blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures.

Parents are advised that a determined user may be able to gain access to online content and/or apps/services that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to content that they and/or their parents may find inappropriate, offensive, objectionable, or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

Principals are responsible for providing training so that students under their supervision are knowledgeable about this policy and its accompanying guidelines.

Pursuant to Federal law, students shall receive education about the following:

A. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;

B. the dangers inherent with the online disclosure of personally identifiable information;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying, and other unlawful or inappropriate activities by students online; and

D. unauthorized disclosure, use, and dissemination of personally-identifiable information ("PII") regarding minors.

Staff members shall provide guidance and instruction to their students regarding the appropriate use of District Information & Technology Resources and online safety and security as specified above. Additionally, such training shall include, but not be limited to, education concerning appropriate online behavior including interacting with others on social media, including in chat rooms, and cyberbullying awareness and response. Furthermore, staff members will monitor, in accordance with Federal and State law, the online activities of students while they are at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions or use of specific monitoring tools to review browser history and network, server, and computer logs. The District will provide parents with appropriate notice – to the extent required by State law – when such monitoring takes place.

All students who use District Information & Technology Resources (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines. See Form 7540.03

F1.
In order to keep District Information & Technology Resources operating in a safe, secure, efficient, effective, and beneficial manner to all users, students are required to comply with all District-established cybersecurity procedures including, but not limited to, the use of multi-factored authentication for which they have been trained. Principals are responsible for providing such training on a regular basis and measuring the effectiveness of the training.

Students will be assigned a District-provided school email account that they are required to use for all school-related electronic communications, including those to staff members, peers, individuals, and/or organizations outside the District with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned e-mail account when signing-up/registering for access to various apps/services.

Students are responsible for good behavior when using District Information & Technology Resources – i.e., behavior comparable to that expected of students when they are in physical classrooms and school buildings and at school-sponsored events. Because communications on the Internet are often public in nature, general school rules for behavior and communication apply. The Board does not approve any use of its Information & Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Students may only use District Information & Technology Resources to access or use social media if it is done for educational purposes in accordance with their teacher's approved plan for such use.

Use of Artificial Intelligence Tools For School Work

To ensure the integrity of the educational process and to promote fair and equal opportunities for all students, except as outlined below, the use of Artificial Intelligence (AI) tools is strictly prohibited for the completion of school work. The use of AI tools, without the express permission/consent of a teacher, undermines the learning and problem-solving skills that are essential to academic success and that the staff is tasked to develop in each student. Students are encouraged to develop their own knowledge, skills, and understanding of course material rather than relying solely on AI tools and they should ask their teachers when they have questions and/or need assistance. Unauthorized use of AI tools is considered a form of plagiarism, and any student found using these tools without permission or in a prohibited manner will be disciplined in accordance with the Student Code of Conduct. (See Policy 7540.09 - Artificial Intelligence ("AI"))

Notwithstanding the preceding, students can use AI tools in the school setting if they receive prior permission/consent from their teacher, so long as they use the AI tools in an ethical and responsible manner. Teachers have the discretion to authorize students to use AI tools for the following uses:

A. Research assistance: AI tools can be used to help students quickly and efficiently identify background information, including locating relevant information and sources for their school projects and assignments, suggesting research questions, providing opposing viewpoints, identifying blind spots, and suggesting other perspectives.

B. Data Analysis: AI tools can be used to help students with pattern identification and to analyze, understand, and interpret large amounts of data, such as text documents or social media posts. This can be particularly useful for research projects or data analysis assignments – e.g., scientific experiments and marketing research.

C. Language translation: AI tools can be used to translate texts or documents into different languages, which can be helpful for students who are learning a new language or for students who are studying texts written in a different language. AI tools can also remove abstract language from a text, adjust text complexity, and provide background information about a culture to help a student understand texts.

D. Writing assistance: AI tools can provide feedback on a student's writing, including grammar and spelling corrections, as well as suggest alternative word choices and sentence structure, to help students improve their writing skills. Similarly, AI tools can offer suggestions to modify tone and voice, organize a student's thinking, identify bias, suggest additional topics, and ask questions to expand the student's thinking on a topic.

E. Accessibility: AI tools can be used to help students with disabilities access and understand written materials. For example, text-to-speech software can help students with specific learning disabilities or visual impairments to read texts and AI-powered translation tools can help students with hearing impairments understand spoken language (e.g., create transcripts or provide closed-captioning for spoken material).

When AI tools are used responsibly and effectively, they can supplement, not replace, traditional learning methods. If a student has any questions about whether they are permitted to use AI tools for a specific class assignment, they should ask their teacher.

In accordance with their teacher's direction, students are required to cite/identify work generated/created with the use of AI tools and explain/demonstrate how the AI tools were used in the creation of the work.
Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District Information & Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and Principals as the administrator(s) responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District Information & Technology Resources.

DISTRICT-ISSUED STUDENT E-MAIL ACCOUNT

Students assigned a school e-mail account are required to utilize it for all school-related electronic communications, including those to staff members and individuals and/or organizations outside the District with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school assigned e-mail account when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.

This policy and any corresponding guidelines serve to establish a framework for student's proper use of e-mail as an educational tool.

Personal e-mail accounts on providers other than the District's e-mail system may be blocked at any time if concerns for network security, SPAM, or virus protection arise. Students are expected to exercise reasonable judgment and prudence and take appropriate precautions to prevent viruses from entering the District's network when opening or forwarding any e-mails or attachments to e-mails that originate from unknown sources.

Students shall not send or forward mass e-mails, even if educationally-related, without prior approval of their classroom teacher or the Technology Director and/or site administrator.

Students may join list servs or other e-mail services (e.g. RSS feeds) that pertain to academic work, provided the e-mails received from the list servs or other e-mail services do not become excessive . If a student is unsure whether s/he has adequate storage or should subscribe to a list serv or RSS feed, s/he should discuss the issue with his/her classroom teacher, the building principal or the District's Technology Director. The Technology Director and/or site administrator is authorized to block e-mail from list servs or e-mail services if the e-mails received by the student becomes excessive.

Students are encouraged to keep their inbox and folders organized by regularly reviewing e-mail messages and purging e-mails once they are read and no longer needed for school.

Unauthorized E-mail

The Board does not authorize the use of its Technology Resources, including its computer network ("network"), to accept, transmit, or distribute unsolicited bulk e-mail sent through the Internet to network e-mail accounts. In addition, Internet e-mail sent, or caused to be sent, to or through the network that makes use of or contains invalid or forged headers, invalid or non-existent domain names, or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit e-mail to be sent to or through the network is unauthorized. Similarly, e-mail that is relayed from any third party's e-mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the e-mail, is also an unauthorized use of the network. The Board does not authorize the harvesting or collection of network e-mail addresses for the purposes of sending unsolicited e–mail. The Board reserves the right to take all legal and technical steps available to prevent unsolicited bulk e-mail or other unauthorized e-mail from entering, utilizing, or remaining within the network. Nothing in this policy is intended to grant any right to transmit or send e-mail to, or through, the network. The Board's failure to enforce this policy in every instance in which it might have application does not amount to a waiver of its rights.

Unauthorized use of the network in connection with the transmission of unsolicited bulk e-mail, including the transmission of counterfeit e-mail, may result in civil and criminal penalties against the sender and/or possible disciplinary action.

Authorized Use and Training

Pursuant to Policy 7540.03, students using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use and safety by signing and submitting Form 7540.03 F1 annually.

Furthermore, students using the District's e-mail system shall satisfactorily complete training , pursuant to Policy 7540.03, regarding the proper use of e-mail .

PERMISSION-SIGNATURE PAGE

Parents/Guardians : Co-sign with your student. After completing, please promptly return.

Student User's Full Name (please print): _____

School:_____ Grade: _____

Parent/Guardian's Name: _____

Parent/Guardian

As the parent/guardian of this student, I have read the Student Technology Acceptable Use and Safety Policy and Guidelines, and have discussed them with my child. I understand that student access to the Internet is designed for educational purposes and that the Board has taken available precautions to restrict and/or control student access to material on the Internet that is obscene, objectionable, inappropriate and/or harmful to minors. However, I recognize that it is impossible for the Board to restrict access to all objectionable and/or controversial materials that may be found on the Internet. I will not hold the Board (or any of its employees, administrators or officers) responsible for materials my child may acquire or come in contact with while on the Internet. Additionally, I accept responsibility for communicating to my child guidance concerning his/her acceptable use of the Internet - i.e., setting and conveying standards for my daughter/son to follow when selecting, sharing and exploring information and resources on the Internet. I further understand that individuals and families may be liable for violations. To the extent that proprietary rights in the design of a web page, site, service or app hosted on Board-owned or District-affiliated servers would vest in my child upon creation, I agree to assign those rights to the Board.

Please check each that applies:

____I give permission for the Board to issue an e-mail account to my child.
____I give permission for my child's image (photograph) to be published online, provided only his/her first name is used.
____I give permission for the Board to transmit "live" images of my child (as part of a group) over the Internet via a web cam.
____I authorize and license the Board to post my child's class work on the Internet without infringing upon any copyright my child may own with respect to such class work. I understand only my child's first name will accompany such class work.

Parent/Guardian's Signature: _____ Date: _____

Student

I have read and agree to abide by the Student Technology Acceptable Use and Safety Policy and Guidelines. I understand that any violation of the terms and conditions set forth in the Policy and Guidelines is inappropriate and may constitute a criminal offense and/or may result in disciplinary action. As a user of District Technology Resources, I agree to communicate over the Internet and through the Technology Resources in an appropriate manner, honoring all relevant laws, restrictions and guidelines.

Student's Signature: _____ Date: _____

Teachers and building principals are responsible for determining what is unauthorized or inappropriate use. The principal may deny, revoke or suspend access to and use of the Technology Resources to individuals who violate the Board's Student Technology Acceptable Use and Safety Policy and related Guidelines, and take such other disciplinary action as is appropriate pursuant to the Student Code of Conduct.