

Fort Sam Houston Independent School District

Student Responsible Use Agreement for Technology Resources

To prepare students for an increasingly technological society, the district has invested in using district-owned technology resources for instructional purposes. As a result, specific resources may be issued to students. These specialized resources, including the district's network systems and use of district equipment, are restricted to approved purposes only. Violations of this user agreement may result in withdrawal of privileges and disciplinary action.

Unacceptable and Inappropriate Use of Technology Resources

- Sending, possessing, or posting electronic messages, videos, audio recordings, or images that are abusive, obscene, sexually oriented, harassing, threatening, intimidating, illegal, or that cause a material or substantial disruption at school, including cyberbullying (*See CIPA definitions at the end of this document for further details*)
- Using any device or technology to copy or capture an image or the content of any District materials (such as tests or exams) without permission of a teacher or administrator
- Making, participating in the making of, transmitting to another via an electronic device, or posting to the Internet a digital, video, or audio recording or image of an actual or simulated act that involves a crime or conduct prohibited by the Student Code of Conduct
- Using any device or technology to record the voice or image of another in any way that disrupts the educational environment, invades the privacy of others, or without the prior consent of the individual recorded.
- Using any device or technology to record the voice or image of another to take or electronically falsify an image (deepfake) to disseminate, transfer, circulate, exhibit, present, or share audio, images, video, or photos that reveal private parts of the body that are normally covered by clothing (a.k.a. sexting)
- Using the name, persona, or image of another student, District employee, or volunteer to create a web page or post one or more messages on a website without the other person's consent.
- Using email, websites, or electronic devices to engage in or encourage illegal conduct, violate the Student Code of Conduct, or threaten school safety.
- Attempting to or successfully accessing or circumventing passwords or other security-related information of the District, officials, volunteers, employees, or other students by any means
- Attempting to or successfully altering, destroying, interrupting, intercepting, or disabling district technology equipment, district data, the data of other users of the district's computer system, or other networks connected to the district's system, including uploading or creating computer malware
- Attempting to or successfully accessing proxy services, including but not limited to proxy websites, to circumvent district filtering
- Copying, downloading, reproducing, distributing, retransmitting, redisplaying, or modifying items from the District's website
- Engaging in any of the above forms of technological misconduct outside of school when such conduct causes material or substantial disruption at school as determined by school officials

Safety of Self and Others

- Students should report to their teachers or other school personnel any message received that is inappropriate or makes them feel uncomfortable.
- Students should not reveal personal information about themselves or others or agree to meet with someone they met online without parental knowledge and participation.
- Students must use appropriate language for the educational environment and for the educational activity in which they are currently involved (no swearing, vulgarity, ethnic or racial slurs, or any other inflammatory or threatening language)

Access and Uses

- Students may not send messages under a false identity
- Students may not access email, files, and/or other documents of other users without permission

- Students may not access websites that contain inappropriate or illegal material, including those that have content that is pornographic or sexual in nature, from any computer or other technological device on school property
- Students may not use the internet for financial gain, political or commercial activity; or use the system for illegal purposes or any other activity prohibited by District policy
- Students may not use the system for purchasing products or services

Copyright Laws

- Students must comply and be aware of all copyright laws and follow the copyright laws.

System Security

- Students may not attempt to harm equipment, materials, or data
- Students may not knowingly infect a computer or network with a virus
- Students should always report any violations of the FSHISD Acceptable Use Guidelines to a teacher or administrator

Artificial Intelligence

- Students may not plug in a prompt into an AI tool, copy the response, and submit it as their own
- Students may not copy text or images from AI programs without proper attribution.
- Students may not use AI text or images without fact-checking and exploring potential plagiarism issues.
- Students may not use AI when their teacher expressly forbids it.

Internet Access

We live in a global and digital world -- a world changed by technology and new ideas about how we communicate with one another. FSHISD realizes that students must develop the research, information fluency, and technology skills that will enable them to be successful in this digital world and the skills necessary to live safely and ethically. For this reason, the District provides access to the Internet for all students.

Under the federal Children's Internet Protection Act (CIPA), the district must filter Internet access and teach online safety. In FSHISD, we take your child's security and privacy very seriously. Therefore, the District makes every effort to supervise and monitor student technology use, and we use several filtering appliances to block access to Internet content that is obscene, pornographic, and harmful to minors.

Parents or guardians can terminate their child's internet access by contacting the District Director of Technology. Parents should understand that in doing so, they may prevent their child from accessing Internet-based instructional materials, assessments, and activities that will be available to other students. The District will provide alternative activities for children whose parents do not wish to access the Internet; however, the District cannot ensure that these activities will provide the same richness and depth of experience that access to the Internet can provide.

Account Management of Web-based Services and COPPA

Following our district mission, goals, and vision for technology, students may be issued accounts in third-party systems (e.g., Google Workspace for Education, WeVideo, SeeSaw, Remind, etc.) that are managed by the district. These accounts will be used at school for school-related projects but may also be accessed outside of school and are essential to achieving instructional objectives.

Regarding COPPA (the Children's Online Privacy Protection Act), the school district will decide whether a particular site's or service's information practices are appropriate before issuing student accounts. In cases where students are under 13, district personnel will act in *loco parentis* and will provide consent for the students to use the services in educational contexts. Fort Sam Houston ISD will maintain an approved software library which includes a curated list of reviewed software that may be used instructionally. This approved software library can be accessed on our district website under the Technology Department.

Personal Electronic Devices

Fort Sam Houston ISD highly recommends students utilize the district-issued device. This device provides a secure, consistent, and education-focused environment. District-issued devices are configured with security features and necessary content filters to follow the Children's Internet Protection Act (CIPA) requirements. District-issued devices are configured with security features and necessary content filters.

In some cases, students may find it beneficial or be encouraged to use personal telecommunications or other electronic devices for instructional purposes while on campus.

- When students are not using the devices for approved instructional purposes, devices should be out of sight and not used. Violations of the user agreement may cause withdrawal of privileges and other disciplinary action.
- The possession and use of laptops, tablets, smartphones, cameras, and other electronic communications devices by a student of FSHISD on school property or at school-related events is a privilege and not a right.
- Students must adhere to the Responsible Use Agreement when using these devices.
- The District will not provide technical support for personal devices. Personal devices will not connect to the district network.
- Classroom teachers will establish standards for school-issued and personal device use in their respective classrooms.
- If a student inappropriately uses a personal electronic device, they will lose their privilege of bringing the device to school. Moreover, district administration may impose additional consequences based on the Student Conduct Code.
- The District reserves the right to examine personal electronic devices and search its contents if there is a reason to believe that school policies, regulations, or guidelines have been violated.

Consequences for Inappropriate Use of School-Owned or Personal Technology Resources

- Suspension of access to the District's Electronic Communications System
- Revocation of the District's Electronic Communications System account(s) and/or
- Other appropriate disciplinary or legal action in accordance with the Student Code of Conduct and applicable laws.

NOTE: Students will not be disciplined for technological misconduct related to possessing items described above so long as the student (1) did not contribute to the creation of the item in any way, (2) possessed it only after receiving the item unsolicited from another, (3) either promptly destroyed the item or reported it to a school employee as soon as possible, and (4) did not provide a copy, forward, or re-post the item to anyone other than law enforcement, a school employee, or the student's parent/guardian.

CIPA Definitions of Terms

MINOR. The term "minor" means any individual who has not attained the age of 17 years.

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in section 1460 of title 18, United States Code;
2. Child Pornography, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

HARMFUL TO MINORS. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. 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
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.