Falls City Independent School District
Student Responsible Use Policy

To prepare students for an increasingly technological society, the district has invested in using district-owned technology resources for instructional purposes. 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. Access to FCISD devices and systems is not a right but a privilege and should be treated as such.

Account Management of Web-based Services and COPPA .

Following our district mission, goals, and vision for technology, students may be issued or find it beneficial to create accounts in third-party systems (e.g., Google Workspace for Education, Classlink, St Math, etc.). Such accounts will give students access to FCISD systems, internet, email (7th-12th grade), and third party applications. These accounts will be used at school for school-related projects but may also be accessed outside of school with parent permission 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. Falls City ISD will maintain an approved software library that 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.

Internet Access.

Falls City ISD 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. 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.

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.
- 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.
- Using technology to tease or bully another person.
- 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
- No software of any type may be downloaded, or installed on any district device without knowledge of the Director of Technology
- Participation in any chat room, message board, or news group is prohibited without authorization from a teacher or administrator.
- 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 electronic communications received that are inappropriate or make them feel uncomfortable.
- If a student is uncertain about whether a specific activity is permitted or appropriate, they will ask a teacher or administrator before engaging in that activity.
- 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).
- Students who identify a security problem (Filter, account compromise, etc) should notify a teacher and the Director of technology immediately.
- Students should not reveal their account password or allow another person to use their account. If you suspect that another person is using your account, then notify a teacher or administrator.
- Students are owners of their account, and with that are responsible for all activity initiated by and/or performed under their account.
- Training will be provided for each individual needing to use our computer system and its resources. Ask for assistance if you find yourself unfamiliar with the tools you need to use. The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

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.

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 log-in to use a computer, and log-out to minimize risk of another user using their account.
- Under certain conditions, your account could be deleted and a new one created to help mitigate potential problems.

Personal Electronic Devices/BYOD.

Falls City 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.

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. Such use of a personal device is optional and students will not be penalized for not having a personal device. FCISD is not responsible for damage or theft of personal devices. FCISD is not responsible for any data and/or SMS/MMS charges, or other charges incurred by students during school-related use.

- Students must adhere to the Responsible Use Agreement, student code of conduct, internet acceptable use, or board policies when using devices.
- School internet/network filters will be applied to a device that is connected to the FCISD network. Any attempt to bypass the filter is prohibited.
- 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.
- FCISD is not responsible for the content accessed by users who connect via their own data plans or other methods off of FCISD networks.
- Devices may only be used for school related activities. Games are not permitted, unless otherwise allowed by a teacher or administrator.

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

- Any violation of the above mentioned may result in disciplinary action in accordance with the Student Code of Conduct.

CIPA Definitions of Terms - can be found on the Falls City ISD website.

Responsible Use Agreement.

By signing and returning this document, I give to Falls City ISD to create and manage third party accounts (including but not limited to: Google Workspace apps, Classlink, Adobe, etc) for my child.

I have read the district's technology Responsible use policy and agree to abide by their provisions.

Student signature: _____

Parent signature: _____

Date: _____

.