Fremont Community Schools

2018-2019
Technology Acceptable Use Policy

INTERNET/NETWORK USE

The Internet/Network shall be used by the student or staff member for school-appropriate activities and the user shall be held responsible for his or her conduct. Fremont Community Schools and its employees are not responsible for any damage that may occur due to inappropriate use of the Internet or unwanted financial obligations that could result in goods or services purchased via the Internet by the user.

The use of the Internet to create, change, administer, cyber bully, or visit personal web blogs or personal websites (Facebook,Twitter, etc.) personal email, is strictly prohibited. If inappropriate conduct is noticed, it is the responsibility of the witness to report it to school personnel.

Fremont Community Schools recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyberbullying. Therefore, students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

Inappropriate use of the Internet access and/or Network will result in disciplinary action that could include, but is not limited to, any of the following; loss of Internet/Network use, suspension, expulsion, financial reimbursement, and criminal action. Inappropriate use outside of the school setting may also result in disciplinary action should it disrupt the school process or purpose.

Inappropriate use includes, but is not restricted to:

- Using the Internet/Network for commercial advertising;
- Using copyrighted material in reports without permission or downloading material without permission if needed;
- Using the Internet/Network to lobby for votes;
- Using the Internet/Network to send or receive messages that are discriminatory or

abusive in any manner. (See Cyber Bullying in this handbook.)

- Using the Internet/Network to send or receive messages that contain obscenities or obscene pictures;
- Using the Internet/Network to send or receive messages that are racist and/or sexist, or viewed as bullying, cyber bullying, threatening, and/or harassment;
- Using the Internet/Network to provide information that other may use inappropriately;
- Using the Internet/Network to send or receive inflammatory messages;
- Creating and/or using a computer virus and exposing or attempting to expose it to any computer and/or the Network;
- Using the Internet/Network to send or receive a message with someone else's name on it or access another person's materials, information or files without the direct permission of that person or to give your access information to anyone else;
- Using the Internet/Network to send or receive a message that is inconsistent with the school's code of conduct;
- Accessing the Internet/Network from an unauthorized or unsupervised station;
- Using the Internet/Network and/or computer to do damage, vandalize or disable the property of another person or organization;
- Using the Internet/Network to violate any local, state or federal statute.

All system users have a very limited privacy expectation in the contents of their files on the system and are considered discoverable. Web Pages on this system must meet with the Building Principal's and Technology Coordinator's approval. Links to corporation maintained Web Pages must be made by the Technology Coordinator after receiving the appropriate approvals.

TECHNOLOGY ACCEPTABLE USE POLICY

Introduction

Fremont Community Schools (hereafter, "the School") recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, we provide access to technologies for student and staff use.

This Acceptable Use Policy outlines the guidelines and behaviors that users are

expected to follow when using school technologies or when using personally-owned devices on the school grounds including school buses.

- The School's network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored and retained.
- **Access to online content via the network may be restricted in accordance with our policies and federal regulations,**
  such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- **Misuse of school resources may result in disciplinary action.**
- The School makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users, *both students and staff,* of the district network or other technologies are expected to alert IT staff immediately
  of any concerns for safety or security.

Technologies Covered

The School may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

As new technologies emerge, the School will attempt to provide access to them. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

The School provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow district protocol to alert an IT staff member or submit the site for review.

Email

Fremont Community Schools will provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, the School will provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

- Fremont Community Schools utilizes a number of computer and web-based tools for learning. Since these tools are provided by third parties, COPPA Regulations require that we obtain parental permission for use of such tools.
- Under Federal COPPA law, these websites must notify parents and obtain parent consent before collecting personal information from a child under the age of 13. However, the law does permit schools to consent to the collection of personal information on behalf of the students. This in turn eliminates the need for parental consent.
- Your signature on this Acceptable Use Policy constitutes your consent in allowing Fremont Community schools to provide the following personal identifying information to third party web-based applications. This information is used in creating student accounts for GSuite, which allows the students to use Chromebook devices at school.
    - First Name
    - Last Name
    - Email address
    - Username

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices Policy

The School may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to school staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices off the school network may be monitored.

Personally-Owned Devices Policy

Students should keep personally-owned devices (including laptops, tablets, smartphones, and cell phones) turned off and put away during school hours unless in the event of an emergency or as instructed by a teacher or staff for educational purposes.

Because of security concerns, when personally-owned mobile devices are used on campus, they should not be used over the school network without express permission from IT staff. In some cases, a separate network may be provided for personally- owned devices.

Search and Seizure

Student network accounts are not private accounts. Monitoring systems are in place per CIPA regulations to keep our students safe. In some cases these systems uncover behavior that violates this policy or law. In such cases the Technology Director and Administration will conduct searches if there is reasonable suspicion and/or evidence to warrant it, or if requested by local, state, or federal officials.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. The use of a login by someone other than the user is forbidden and is grounds for limitations to mobile device or computer access.

If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run .exe programs over the school network or onto school resources without express permission from IT staff.

You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, and only for education purposes.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there--and can sometimes be shared and spread in ways the user never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if at school; parent if using the device at home) immediately.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Examples of Acceptable Use

User will:

- ./ Use school technologies for school-related activities.
- ./ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- ./ Treat school resources carefully, and alert staff if there is any problem with their operation.
- ../ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- ./ Alert a teacher or other staff member if user sees any threatening, inappropriate, or harmful content (images, messages, posts) online.
- ./ Use school technologies at appropriate times, in approved places, for educational pursuits.
- ../ Cite sources when using online sites and resources for research.
- ./ Recognize that use of school technologies is a privilege and treat it as such.
- ./ Be cautious to protect the safety of myself and others.
- ./ Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use

User will **not:**

- ./ Use school technologies in a way that could be personally or physically harmful.
- ./ Attempt to find inappropriate images or content.
- ./ Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- ./ Try to find ways to circumvent the school's safety measures and filtering tools.
- ./ Use school technologies to send spam or chain mail.
- ./ Plagiarize content found online.
- ./ Post personally-identifying information, about myself or others.
- ./ Agree to meet someone met online in real life.
- ./ Use language online that would be unacceptable in the classroom.
- ../ Use school technologies for illegal activities or to pursue information on such activities.
- ../ Attempt to hack or access sites, servers, or content that isn't intended for user.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

The School will not be responsible for damage or harm to persons, files, data, or hardware.

While the School employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

The School will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Suspension from school and school-related activities
- Legal action and/or prosecution