

Fruitport Community Schools

Acceptable Use Policy and User Agreement for FCS Technology Resources Staff Form

The purpose of this policy is to define acceptable use of Fruitport Community Schools (FCS) Technology Resources by FCS employees, Board members, and other individuals other than students.

The use of the FCS Technology Resources is a privilege that may be monitored at any time to ensure adherence to accepted ethical and legal standards and practices.

“FCS Technology Resources,” and other related terms (specifically those underlined below), are defined in more detail on the attached AUP Reference document.

In exchange for the use of FCS Technology Resources either at school or away from school, the user understands and agrees to the following:

1. Misuse of FCS Technology Resources may result in suspension of account privileges and/or other disciplinary action, up to and including termination of employment.
2. The user shall have no expectations of privacy when using any FCS Technology Resources, including professional or personal communications. FCS reserves the right to retrieve, examine and duplicate computer files, remove content, restrict use, or revoke access to FCS Technology Resources at any time, for any reason.
3. FCS reserves the right to monitor mail space and file server utilization.
4. The user will abide by FCS password protection and confidentiality requirements.
5. As soon as possible, users shall disclose to their supervisor any message received that is inappropriate or makes the user feel uncomfortable, harassed, threatened, or bullied, especially any communication that contains sexually explicit content. Content of this nature should not be deleted until instructed to do so by an immediate supervisor.
6. FCS Technology Resources may not be used for commercial purposes, with the exception of the Classified Ads e-mail list, or to personally lobby or solicit political positions or candidates.
7. Employees are prohibited from using FCS Technology Resources to facilitate unprofessional/inappropriate personal relationships with students.
8. The user may not use FCS Technology Resources or any other communication/messaging devices to engage in harassment or cyberbullying.
9. FCS staff is responsible for using social media in a way which represents them in a professional manner.
10. While working with students, FCS staff members are required to monitor student technology access in order to adhere fully with CIPA compliance laws. Students under the age of 13 may not create online accounts due to COPPA restrictions. Filters and other network security features may be disabled by authorized FCS personnel to enable access for research or other acceptable purposes.
11. Users may not copy or transfer software belonging to FCS without the permission of the FCS Director of Technology or his/her designee. Without first obtaining such permission, the user will be liable for any damages and will be required to pay the cost of any damages, whether intentional or accidental.

12. FCS staff may not load software on any FCS Technology Resources without permission of the FCS Director of Technology Services or his/her designee and must use appropriate software ordering procedures.
13. Before using a district owned iPad, users must read and sign the Acceptable Use Policy and User Agreement specific to iPads and must follow specific guidelines regarding proper care and application purchase.
14. The user is responsible for the proper use of FCS Technology Resources and will be held accountable for any damage to, or replacement of, said resources if damage is caused by inappropriate use.
15. The user is solely responsible for all charges and fees, including outside telephone, printing, and merchandise purchases made using FCS Technology Resources for personal use. FCS is not a party to such transactions and shall not be liable for any costs or damages, whether direct or indirect.
16. The user acknowledges and understands that correspondence sent or received over the FCS's network may be subject to retrieval under the State of Michigan Freedom of Information Act (FOIA), MCL 15.231 – 246. The user agrees to cooperate fully and promptly with the FCS when responding to FOIA requests concerning communications over the FCS's computer network.
17. The user acknowledges that they may receive or have access to student education records and other data subject to confidentiality requirements of the Family Educational Rights and Privacy Act (FERPA), 20 USC § 1232g, Individuals with Disabilities Education Act (IDEA), the Michigan Mandatory Special Education Act (MMSEA), and the National School Lunch Act and their underlying regulations (collectively, the "Acts"). You acknowledge that, to the extent you receive and have access to such data and records, you are subject to the provisions of those Acts and their regulations, and will not re-disclose student data or other education records except as permitted by law.

Addendum - AUP Reference Pages

FCS Technology Resources

FCS Technology Resources include, but are not limited to: (1) internal and external network infrastructure, (2) Internet and network access, (3) computers, (4) tablets, (5) iPads, (6) servers, (7) storage devices, (8) peripherals, (9) software, and (10) messaging or communication systems.

Password Protection and Confidentiality Requirements

The user is responsible for accounts, passwords, and any access gained to FCS Technology Resources using the account and password. Any problems arising from the use of the account/password is the responsibility of the user. Use of the account by someone other than registered user is not allowed and may be grounds for loss of access and other disciplinary consequences. This may include termination for both the user and the person(s) using the account and password. The user is required to immediately report any loss, apparent theft, or unauthorized use of the the user's password and must immediately report any apparent transactions attributable to the use of lost or stolen password.

Children's Internet Protection Act (CIPA) and Children's Online Privacy Protection Act (COPPA)

FCS is supported by federal funds which require users to monitor online activities of its minor students and provide technology protection measures on its computers with Internet access designed to prevent minors from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. Students under the age of 13 may not create online accounts due to restrictions of the Children's Online Privacy Protection Act.

Cyberbullying

Cyberbullying means "...the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others." [Definition written by Bill Belsy, available at <http://www.cyberbullying.org>.]

Freedom of Information Act (FOIA)

State of Michigan Freedom of Information Act (FOIA), MCL 15.231 – 246 - "It is the public policy of this state that all persons, except those persons incarcerated in state or local correctional facilities, are entitled to full and complete information regarding the affairs of government and the official acts of those who represent them as public officials and public employees, consistent with this act. The people shall be informed so that they may fully participate in the democratic process." *This means that someone can make a request of copies of the documents or email you have created using FCS Technology Resources.*

Using Social Media

Free speech protects educators who want to participate in social media, but the laws and courts have ruled that schools can discipline employees if their speech, including online postings, disrupts school operations. FCS encourages employees to participate in online social activities; however, it is important to create an atmosphere of trust and individual accountability, keeping in mind that information produced by FCS employees is a reflection on the entire district and is subject to the district's *Acceptable Use Policy*.

Appropriate Use of Social Media

Employees are responsible for the content they publish online. Employees who post to social media sites such as Facebook, MySpace and YouTube which includes inappropriate information such as, but not limited to, provocative photographs, sexually explicit messages, use of alcohol, drugs or anything students are prohibited from doing, must understand that if students, parents or other employees obtain access to such information, their case will be investigated by school administrators. Courts have ruled that schools can discipline employees if their actions, including online postings, distract from or disrupt the educational process. Discipline may include suspension and/or other disciplinary action, up to and including termination of employment.

Employees should be aware that their online communications are date/time stamped. Use of social media should be limited to school-related business during working hours.

The lines between public and private, personal and professional are blurred in the digital world. Even when you have a disclaimer or use a different user name, you will always be considered to be a district employee. Whether it is clearly communicated or not, you will be identified as working for and sometimes representing the organization in what you do and say online. For this reason it is important for FCS employees to read and understand the MAISD's "Social Media Best Practices for Employees" document. Sound judgment and due care should be exercised when using social media outside of the organizational setting.

Personal Relationships with Students

Employees are prohibited from establishing unprofessional, inappropriate personal relationships with students. Examples of unprofessional relationships include, but are not limited to: employees fraternizing or communicating with students as if employees and students were peers such as writing personal letters or e-mails; "texting" students; calling students on cell phones or allowing students to make personal calls to them unrelated to homework or class work; sending inappropriate pictures to students; discussing or revealing to students personal matters about their private lives or inviting students to do the same (other than professional counseling by a school counselor); and engaging in sexualized dialogue, whether in person, by phone, via the Internet, or in writing

Misuse of Technology Resources

Misuse of technology resources, includes, but is not limited to:

1. Accessing or attempting to access educationally inappropriate materials/sites, including, without limitation, material that is unlawful, obscene, pornographic, profane, or vulgar. The determination of a material's "appropriateness" is based on both the material's content and intended use.
2. Cyberbullying (as defined above) or any other use of the Technology Resources that would violate FCS's anti-bullying rules or policies. Cyberbullying may, without limitation, include posting slurs or rumors or other disparaging remarks about another person on a website; sending email or instant messages that are meant to threaten, harass, intimidate, or drive up a victim's cell phone bill; taking or sending embarrassing or sexually explicit photographs, video, or other visual depictions of another person; or posting misleading or fake photographs of others on websites.
3. Sexting, which includes, without limitation, possessing, sending, or distributing nude, sexually explicit, or sexually suggestive photographs, videos, or other visual depictions of yourself or another person over FCS's Technology Resources from any means, including over personally owned devices.
4. Vandalism, which includes, without limitation, any malicious or intentional attempt to harm, steal, destroy, or disrupt user data, school materials, or school hardware; violating the integrity of FCS's Technology Resources; uploading or creating viruses; downloading/installing unapproved, illegal, or unlicensed software; or seeking to circumvent or bypass security measures.
5. Hacking, which includes, without limitation, gaining or attempting to gain access to, modifying, or obtaining copies of, unauthorized information or information belonging to other users.
6. Unauthorized copying or use of licenses for copyrighted software.
7. Plagiarizing, which includes the unauthorized distributing, copying, using, or holding out as your own, copyrighted material (most of the Internet is copyrighted), or material written by someone else, without permission of, and attribution to, the author.
8. Misrepresenting others, including, without limitation, posting confidential or inappropriate information (text, video, photo) meant to harass, intimidate, or embarrass students or staff on any social media network or website.
9. Allowing anyone else to use a password-protected account.
10. Using or soliciting the use of, or attempting to use or discover the account information or password of, another user.
11. Attempting to or successfully disabling security features, including technology protection measures required under the Children's Internet Protection Act (CIPA).
12. Misusing equipment or altering system software without permission.
13. Establishing connections which create routing patterns that are inconsistent with the effective and shared usage of the network.
14. Commercial for-profit activities, advertising, personal political lobbying, or sending personal mass mailings or spam.
15. Using the Technology Resources in any way that violates any federal, state, or local law or rule.

Fruitport Community Schools

*Acceptable Use Policy and User Agreement for FCS Technology Resources
Staff Signature Form*

In consideration for the privileges of using the FCS’s Technology Resources and in consideration for having access to the information contained therein, I release the FCS, its Board of Education, individual Board members, administrative employees and agents, and the Internet provider and its operators, from any and all claims of any nature arising from my use, or inability to use, the FCS Technology Resources. I agree to abide by this Acceptable Use Policy and Agreement and by any rules or regulations that may be added from time-to-time by the FCS. I agree to pay for, reimburse and indemnify the FCS, its Board of Education, individual Board members, and administrative employees and agents for damages, including any fees, expenses, liability or other damages of every sort and nature, incurred as a result of my use or misuse of FCS Technology Resources.

All users of FCS Technology Resources shall, by their signature below, agree to abide by all terms of this policy and understand that violation(s) may result in the loss or restricted access to FCS Technology Resources and/or other disciplinary actions in cooperation with the user’s employer and/or school district.

I have read this Acceptable Use Policy and User Agreement for use of Technology Resources and sign it knowingly and freely.

First Name Last Name

Job Title Building

Employee or Agent Signature Date