Fairfield Community School Corporation

Administrative Guidelines and Acceptable Use Agreement For Student Technology

Revision 1.4

Currently Approved by:

Superintendent	Steve Thalheimer
Building Principals	Amy Bertram Nick Jones Carla Hochstetler Lisa Litwiller Dan Sharp Teresa Zook
Technology Coordinator	Andrew England

Published May 2009
Revision 1.1 October 2009
Revision 1.2 April 2011
Revision 1.3 August 2013
Revision 1.4 May 2017

Table of Contents

Overview

The Fairfield Community School Corporation is pleased to offer its Users access to the Internet. Google Apps for Education, other 21st Century Web 2.0 Tools. The Internet and these tools enables staff and students to explore the world through access to thousands of digital resources. The Corporation expects that faculty will blend thoughtful use of the Internet and Web 2.0 tools throughout the curriculum and will provide guidance and instruction to students in how to use them appropriately. As much as possible, access from school to Internet resources should be structured in ways which have been evaluated prior to use. While students will be able to move beyond those resources to others that have not been previewed by staff, they shall be provided with guidelines and lists of resources particularly suited to learning objectives. In making decisions regarding staff access to the FCSC Network and Internet, the Fairfield Community School Corporation considers its own stated educational mission, goals, and objectives. We seek to build a culture of 21st Century learners and leaders who are digitally literate, and able to collaborate and communicate efficiently and effectively using digital tools.

The Corporation believes the benefit of Internet access to all Users exceeds the disadvantages. While the Corporation's intent is to make Internet access available in order to fulfill its educational goals and objectives, Users may find ways to access other materials as well. Users should understand that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, or potentially offensive to people. **FCSC will make every effort to prevent inappropriate information, images and web sites from being accessed** via a content filtering system, but the Corporation makes no implied or expressed guarantee that it will not occur by Users intent on inappropriate access by any means available to them, or that the filter will catch everything that might be deemed inappropriate. In these cases, it should be immediately reported to the Technology Director.

In making decisions regarding student access to the Internet, FCSC will always consider its own educational mission, goals and objectives. Electronic information research skills are now fundamental in preparing citizens and employees. Access to the Internet enables Users to explore libraries, databases and other resources from around the world. For school purposes or educational functions, the service must be used under direct supervision of a faculty/staff member. The Corporation expects the faculty will blend the thoughtful use of the Internet throughout the curriculum and will provide guidance and instruction to Users.

Board Policy Reference: http://www.neola.com/fairfield-in/

Students
5136 – Personal Communication Devices

Property
7540 - Computer Technology and Networks
7540.02 - Corporation Web Page
7540.03 - Student Network and Internet Acceptable Use and Safety
7542 - Access to Corporation Technology Resources from Personal Communication Devices

Use of Corporation Computers/Technology Equipment Guidelines

Corporation computer Users authorized to operate a computer on the Corporation computer network shall be assigned a username and password upon verification of a signed Acceptable Use Agreement (AUA). Each User's password will be changed every 90-days for security reasons, and follow the password policy as stated in the Technology Security Guidelines (page 4).

No User is to use any computer and/or related equipment without proper authorization.
In order to become authorized to use the Corporation's Network, a person must qualify in at least one of the following categories:

- Be an employee of the Corporation with a username, password and signed AUA on file. This includes full and part-time teachers, staff, and administration.
- Student teachers, employees through cooperative agreements, and consultants working with the district will also qualify temporarily upon signing an AUA.
- Be an enrolled student in the Corporation with a username, password and signed AUA on file.
- Be an employee from a technology vendor or consultant providing the Corporation with services.

All others are not authorized Users of FCSC computers unless permission is granted from the Superintendent or District Technology Director.

Computers, Schools and the Indiana Criminal Code

It is important to realize that failure to follow Fairfield Community School Corporation computer technology policies and guidelines may also violate Indiana Criminal Code and be subject to prosecution.

IC 35-43-1-4 Computer Tampering

A person who knowingly or intentionally alters or damages a computer program or data, which comprises a part of a computer system or computer network without the consent of the owner of the computer system or computer network commits computer tampering, a Class D felony.

However, the offense is a:
(1) Class C felony if the offense is committed for the purpose of terrorism

Example: Susie finds her teacher's or fellow student's password and uses it to access his/her account to change grades or delete files. In other words, intentionally changing or deleting any files on the network that are not her own.

IC 35-43-2-3 Computer Trespass

A person who knowingly or intentionally accesses:
(1) a computer system;
(2) a computer network; or
(3) any part of a computer system or computer network;
without the consent of the owner of the computer system or computer network, or the consent of the owner's licensee, commits computer trespass, a Class A misdemeanor.

Example: Any time a student logs in as someone else, without permission of the other person, computer trespass has been committed.

Technology Security Guidelines

FCSC is concerned about protecting information and services from misuse or destruction. The following is a description of steps taken to ensure our devices and systems, the information we have stored in them, and the people who use them are kept safe from harm. Our goals include, but are not limited to:

A. **Prevention**:
This strategy involves providing proper software and/or hardware systems and taking precautions to stop misuse/abuse before it happens. This is supplemental to the adopted FCSC Acceptable Use Agreement. Here are the prevention steps that FCSC takes:

- All Users are required to login only with their assigned, unique username and password. Users may not use another user's login on any device or system. Users may not login to a device or system with their username and password for another user.
- Users are not to share their login information with anyone. Users must not allow someone to "eavesdrop" as they type their password.
- Passwords must be a minimum of eight (8) characters and a combination at least 3 of the following: uppercase alphabetical, lowercase alphabetical, numbers, and special characters such as: "&,*()+=-_&!?.
- Passwords are confidential and must be treated as such.
- All corporation data, specifically confidential information, must be stored on secure network servers. Confidential data must not be stored on local computer drives, thumb drives, and other portable media.
- When and where appropriate, security software may be installed on workstations that allow supervisors to monitor appropriate use and access in real time and/or clear all workstation changes upon reboot.
- Anti-virus software will be installed and automatically updated for all workstations.
- No users are to connect personal electronic devices (such as laptops, MP3 players, etc.) to the network directly or via a district computer because such connections pose a threat to the entire network due to outside viruses or malware. Permission to connect such devices can be sought from the District Director.
    - Students reference Board Policy 5136
- FCSC personnel have the responsibility to guide and monitor their students. No students are to be left unmonitored when using technology.
- Students are only permitted to use the Corporation provided email and to do so for educational purposes. No third-party web-based Email services are to be used by anyone unless authorized by the District Technology Director.

HIPAA - Health Information Privacy
"The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information, and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety." http://www.hhs.gov/ocr/privacy/index.html

FERPA - The Family Educational Rights and Privacy Act
"A Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education." http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

B. **Education**:
This strategy involves helping Users make wise choices when using the internet and promoting ways to use that internet that help educate students. Towards these ends, the district does the following:

- The district maintains a technology intranet site to share resources and information.
- The district provides links to and resources for teaching internet safety to students per E-Rate compliance requirements. As of October 10, 2008, the "Protecting Children in the 21st Century Act" mandates that elementary and secondary schools having computers with Internet access may not receive services at discount rates unless they submit to the Federal Communications Commission a certification that they are "educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and chat rooms and cyber bullying awareness and response."
- The district Curriculum intranet site contains links to multiple classroom and teaching resource sites.
- Professional development is offered in ways to implement technology into the classroom and in ways to use technology for records management and data collection.

Guidelines for 21st Century & Digital Web 2.0 Tools

- In order for FCSC to provide students with the most effective web-based tools for learning, we need to abide by Federal COPPA Regulations that require parental permission. Our school corporation utilizes several computer and web-based apps and services operated not by FCSC, but by third parties. These parties include: The G Suite for Education (formally Google Apps for Education), and other similar educational programs and apps.

- In order for staff and students to use these programs and services, basic personal identifying information, including name, user name, and email address must be provided to the website operator. In many of these cases, access to these websites and resources is provided through a teacher account, and is monitored by the teacher using the resource.

- Under Federal COPPA law, these websites must notify parents and obtain parental consent before collecting personal information from children under the age of 13. However, the law permits schools such as FCSC to consent to the collection of personal information on behalf of all of its students, thereby eliminating the need for individual parental consent given directly to each website provider.

- Your signature on this Acceptable Use Agreement constitutes your consent for FCSC to provide limited personal identifying information consisting of first name, last name, email address, and user name to the following web-operators: G Suite for Education, and the operators of additional web-based educational programs which FCSC may deem necessary during the upcoming academic school year.

- If staff members find new Web 2.0 Tools and/or Apps to use with students, they must check the privacy policies of those web tools to ensure that they meet age restrictions and that they are educationally appropriate.

Technology Donations Guidelines

Fairfield Community Schools recognizes that patrons and/or staff members may wish to donate technology hardware and software to the Corporation. FCSC realizes that under certain circumstances, this is a valuable and appreciated act. FCSC also recognizes that vendors and conferences occasionally provide technology incentives such as computers and projectors that can also provide value to the District. However, the Corporation must set minimum standards for such donations to insure they are capable of supporting our curricular offerings and/or do not require extensive upgrading or proprietary maintenance tasks. In all instances, technology gifts and incentives become the property of Fairfield Community Schools in accord with Board Policy. (Reference Policy 3214 - STAFF GIFTS)

Computers
The Corporation will only accept computers that meet or exceed the following specifications:

Intel i5 Processor
4 GB RAM
120 GB Hard Drive
DVD/DVD-RW ROM Drive

- Systems will need evaluated and approved by the Technology Director for acceptance, to ensure they are in line with current standards and practices for continuity.
- Systems requiring repair will not be accepted except for parts.

Software
The Corporation will accept software under the following conditions:

- The software must be appropriate and useful when integrated into the curriculum as determined by a review of the program by the Director of Curriculum and Technology Director.
- We have assurance that the software is no longer installed on any personal computers in a patron or staff member's home. A signed letter verifying such may be requested.
- All installation disks, manuals, and license agreements must be provided.
- The software is capable of running under MS Windows or other FCSC supported operating system without any adjustments or compatibility alterations.

Other Technology Equipment
The Corporation will accept other technology equipment under the following conditions:

- The technology equipment will need evaluated and approved by the Technology Director for acceptance, to ensure they are in line with current standards and practices for continuity.
- FCSC will not accept old printers, nor will they supply cartridges or support for any outside printers

Due to rapid changes in technology, FCSC reserves the right to adjust the minimum requirements and/or designation of appropriate use of technology donations at any time.

Network and Internet Access Acceptable Use Expectations

The following agreement is in effect for all corporation-provided access to electronic information, services, and networks. All provisions of this document are subordinate to local, state, and federal statute. All students, certified, and non-certified employees are referred to hereafter as User(s) and the Fairfield Community School Corporation is hereafter referred to as the Corporation. The intent of this agreement is to inform all Users and ensure that network policies supported by the Corporation are identified. The network is to be used for educational purposes. As such, the network will assist in the collaboration and exchange of information, facilitate growth through the use of technology, and enhance information gathering and communication skills. All Users are expected to follow the Access Acceptable Use Agreement (AUA) guidelines.

In exchange for the use of Network resources, at school or from a remote location, I understand and agree to the following:

The use of the Network is a privilege, not a right, and may be revoked by the Corporation at any time and for any valid reason. Appropriate reasons include, but are not limited to, the altering of system software; the placing of unauthorized information, viruses or harmful programs on or through the computer system in public or private files or messages; and/or intentional damage to the network. The Corporation reserves the right to inspect and/or remove files, limit or deny access, and refer the User for further disciplinary action. Users will be asked to remove personal files as system storage space becomes low.

The Corporation reserves all rights to any material stored in files which are generally accessible to others and will remove any material which the Corporation, at its sole discretion, believes to be unlawful, obscene, abusive or otherwise objectionable (e.g., graphic violence, the manufacture or use of explosives, weapons, controlled substances, slurs to race, ethnic background, gender, sexual orientation, etc.). Users will not use their Corporation-approved computer account to obtain, view, download or otherwise gain access to, distribute, or transmit such materials.

All information services and features contained in Corporation and Network resources are intended for the private use of its registered Users and any use of these resources for other purposes (e.g., advertisements, political lobbying, for-profit) in any form is expressly forbidden. Use of accounts during school hours should be in support of educational research and/or communication consistent with FCSC educational objectives. Between the hours of 7:30 AM and 3:30 PM, the use of internet for personal reasons should be limited to conserve resources for educational purposes. Internet access should be limited to educationally approved sites. Educationally approved sites are determined by the User with the understanding that he/she may need to justify the site(s) to a peer, administrator, parent, or the public.

The Corporation and Network resources are intended for the exclusive use of its registered Users. The User is responsible for the use of his/her Username, password and any access privileges gained through that account. Any problems arising from the use of an account is the responsibility of the account holder. Use of the account by someone other than the registered account holder is forbidden and may be grounds for further punitive action. Students are not to use staff workstations without prior permission from the staff member.

Any intentional misuse of an account may result in suspension of account privileges and/or other disciplinary action determined by Corporation policies. Misuse is defined as, but not limited to:

Intentionally seeking information on, obtaining copies of, or modifying files, confidential student or personnel records, data, or passwords *belonging to other Users.*

Allowing anyone to access an account other than the registered account holder*.*

Accessing, uploading, downloading, transmitting or distributing pornographic, obscene, or sexually explicit material. Materials containing graphic violence, instruction on the manufacture or use of explosives, weapons, controlled substances, or slurs to race, ethnic background, gender, or sexual orientation is also defined as misuse.

Using the Network and Internet services through malicious hate mail, harassment, profanity, vulgar statements, discriminatory remarks / threats of any kind or "***spoofing",*** i.e., constructing electronic communication so it appears to be from someone else.

Vandalizing, damaging or disabling the property of the Corporation*.* This includes the network, software, computers, monitors, printers, tablets, mobile devices, and all associated equipment.

Violating copyright**,** including downloading, copying or use of licensed or copyrighted software, or otherwise using another person's intellectual property without his/her approval or proper citation.

Failing to use an anti-virus program to scan data source (i.e. cd's, floppies, USB storage drives) prior to use.

Storing executable programs or digital music files in their network home directories or installing software of any kind without permission of the District Technology Director.

Using systems for non-curricular related activity that generates a direct cost to the Corporation.

Violating local, state or federal statutes.

Failing to comply with a direct supervisor's direction**,** especially where that failure constitutes an interference with school purposes or an educational function.

Accessing the Internet while not under direct adult supervision.

Students are prohibited to broadcast, instant message, or chat inside or outside of the FCSC network unless given specific, explicit permission by teacher, Technology Director, or Administrator.

Students' home and personal Internet use can affect the school and other students. If students' personal Internet expression, such as threatening messages or an inappropriate website creates the likelihood of disrupting the school's operations, students may face school discipline and criminal penalties. Students must be aware of the consequences of their communication via social networking (i.e. Facebook, MySpace), learning bulletin boards (i.e. Moodle, Blackboard), and email and text messages.

Sanctions/disciplinary actions shall be dependent upon the severity of the violation. Violations of legal statute will be referred to the proper authorities for investigation. Restitution/ restoration for intentional damages and/or time involved in correcting a situation may be imposed. The Corporation maintains the right to impose sanctions/disciplinary action based upon its own investigation. All Users shall have the right to appeal any decisions/sanctions imposed to the Superintendent or his/her Designee.

The Corporation does not warrant the functions of the system; or guarantee it will meet any specific requirements the User may have or that it will be error-free or uninterrupted. Nor shall the Corporation be liable for any direct, indirect, incidental, or consequential damages that include lost data, information and/or time sustained or incurred in connection with the use, operation, or inability to use the system. The Corporation will not assume responsibility for unauthorized financial obligations obtained through Network use, nor shall the Corporation be liable for the accuracy, nature or quality of information gathered through the Corporation Internet access.

The Corporation will periodically make determinations whether specific uses of the Network are consistent with AUA guidelines and procedures. The Corporation reserves the right to log and track Network usage and monitor server space utilization, including email, by users. The Corporation will not monitor email unless there is an indication of misconduct that is a threat to health and safety or as needed to prevent interference with the academic mission of the Corporation. The Corporation reserves the right to disable/remove a User account to prevent unauthorized activity.

Users are prohibited from downloading programs, installation and/or executable files of any kind without the permission of the Superintendent or Technology Director. Should the User intentionally transfer anything that infects the Network with a virus and causes damage, the User will be liable for any and all repair costs to make the Network fully operational and may be subject to other disciplinary

measures by the Corporation. The User will be liable to pay any costs or fees of any file or software transferred, whether intentional or accidental, without such permission.

There are criminal statutes pertaining to computer tampering (IC 35-43-1-4) and computer trespass (IC 35-43-2-3). Computer tampering deals with knowingly and intentionally altering or damaging a computer program or data without consent and is a Class D felony. Computer trespass deals with knowingly and intentionally accessing a computer system network or a part thereof without consent of the account holder and is a Class A misdemeanor.

FCSC recognizes due process and will follow all local, state, and federal guidelines when applying the corporation AUA.

Email Usage

Email usage guidelines are to discourage disclosure of student and/or administrative information, to comply with all Indiana Public Records laws, and to ensure a safe computing environment for all FCSC Users. Email is defined as any form of electronic mail sent to and from any **student.fairfield.k12.in.us** account. Email service is supplied to students for educational use and the provided service is to be used primarily for that purpose.

- Due to legal implications (HIPAA, FERPA and E-discovery), FCSC students are blocked from accessing personal Email accounts.
- The Email provided by FCSC shall not be used for the creation or distribution of any disruptive or offensive messages, including comments about race, gender, appearance, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, and national origin “chain letters”.
- FCSC Users should have no expectation of privacy in anything they store, send or receive on the FCSC mail system. To ensure compliance, FCSC reserves the right to monitor and inspect email messages for content without notice to the sender or recipient. Such inspections may be conducted at any time, especially if there is a reasonable suspicion that emails from an individual may be criminal, unethical or morally wrong.
- In accord with Federal and State E-discovery laws, FCSC shall backup, store and archive all Email sent and/or received via an FCSC account.
- Any User receiving threatening or unwelcome communications should bring them to the attention of a building Administrator.

Consequences

Malicious misuse of a FCSC account or violation of policies and guidelines may include, but is not limited to, the following sanctions or disciplinary actions:

For Students:

Level 1 Consequence: Up to a 10-day suspension of computer/network privileges and/or limited access to only the necessary educational sites (i.e. Google G Suite, APEX Learning, Read 180, e-textbooks, etc.)

Misuses/Offenses:

- ✓ Use of internet services without adult supervision.
- ✓ Failure to follow a supervisor's instructions.
- ✓ Logging in under another's identity.
- ✓ Storing items on a server other than school-related data.

Level 2 Consequence: Up to a 30-day suspension of computer/network privileges and/or limited access to only the necessary educational sites (i.e. Google G Suite, APEX Learning, Read 180, e-textbooks, etc.)

Misuses/Offenses:

- ✓ Repeat offender from Level 1.
- ✓ Computer usage with no AUP on file.
- ✓ Downloading/installing programs without permission. Examples: chat/
- ✓ messenger services, music players and files, games, wallpaper, etc.
- ✓ Using the Internet to buy, sell or trade items.

Level 3 Consequence: Up to 90-day suspension of computer/network privileges and/or limited access to only the necessary educational sites (i.e. Google G Suite, APEX Learning, Read 180, e-textbooks, etc.)

Misuses/Offenses:

- ✓ Repeat offender from Level 2.
- ✓ Anything that is a threat to the health and safety of others. Examples: hate mail, harassment, threats, etc.
- ✓ Knowingly accessing inappropriate content. Examples: pornography, hacker sites, violent sites, etc.
- ✓ Intentionally bypassing, and/or disabling FCSC security and filtering mechanisms in any way. Some examples, but not limited to, disabling of antivirus software, use of proxy avoidance websites and/or specialized software.
- ✓ Intentionally vandalizing (physically or virtually) technology equipment or software/content.

Level 4 Consequence: Yearlong to permanent suspension of computer/network privileges and/or limited access to only the necessary educational sites (i.e. Google G Suite, APEX Learning, Read 180, e-textbooks, etc.)

Misuses/Offenses:

- ✓ Repeat offender from Level 3.
- ✓ Intentionally accessing corporation systems for the intent of crashing and/or permanently damaging one or more systems.
- ✓ Intentionally accessing confidential systems in violation of HIPAA and/or FERPA.
- ✓ Use of any corporation system for any illegal activity.

Student/Parent Network and Internet Acceptable Use Agreement

The student agrees to abide by the policies, rules and regulations of system usage contained in the FCSC Administrative Guidelines and Acceptable Use Agreement for Student Technology available on the corporation webpage or in hardcopy upon request. The student agrees to follow the rules contained in this document. The student understands that if he/she violates the agreement his/her access can be terminated and he/she may face other disciplinary measures.

Parents/Guardians agree they have read the FCSC Administrative Guidelines and Acceptable Use Agreement for Student Technology available on the corporation webpage or in hardcopy upon request. Parents/Guardians release the district, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from their child/children's use of, or inability to use, the electronic network. This includes, but is not limited to claims that may arise from the unauthorized use of the network components. Parents/Guardians give permission for their child/children to access all components of the district electronic network, which includes Internet access, computer services, videoconferencing, computer equipment and related equipment for educational purposes.

If a parent/guardian wishes for a child to have access to the electronic network and Internet, the form below must be filled out and returned to school within the first two weeks of school starting. If the form is not returned by that point in time, the student will not be allowed to use the district network and Internet.

Student Name: _____

Grade: _____ Teacher Name: _____

Student Signature: _____

Parent/Guardian's Signature_____

Date_____