Cape Fear Center for Inquiry
Policy and Procedure Manual

Series 800 Technology

Table of Contents Page

810	Employee Computer and Internet Use	146
812	Student Internet and Email	149
813	Copyright Compliance	151
814	Student Discipline and Liability	152
816	Access To Services	153
817	Remote Access	154
818	Security Awareness	155
822	Virus Protection	156
824	Network Security	157
825	Internet Safety	158
826	Disaster Recovery	161
840	Hardware and Software Procurement	162
842	Equipment and Material Donations	163
844	Inventory Control	164
846	Equipment Maintenance and Repair	165

810 Employee Computer and Internet Use

The intent of these guidelines is to provide employees with general requirements for utilizing CFCI's computers, networks, and Internet services. These guidelines may be supplemented by more specific administrative procedures and guidelines governing day-to-day management and operation of the computer system.

These guidelines provide general rules and examples of prohibited uses for illustrative purposes but do not attempt to state all required or prohibited activities by users. Employees who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the appropriate administrator.

Failure to comply with this policy and/or the established procedures or rules governing computer use may result in disciplinary action, up to and including discharge. Illegal use of CFCI computers will also result in referral to law enforcement authorities.

A. Access to school computers, networks and Internet services

The level of access that employees have to CFCI computers, networks and Internet services is based upon specific employee requirements and needs.

B. Acceptable use

Employees are to utilize CFCI computers, networks, and Internet services for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted as long as such use does not interfere with the employee's job duties and performance. "Incidental personal use" is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules. **All communications pertaining to any type of school business via e-mail must be performed on the cfci.net account assigned to the employee.**

C. Prohibited use

The employee is responsible for his/her actions and activities involving CFCI's computer, networks and Internet services and for his/her computer files, passwords and accounts. General examples of unacceptable uses which are expressly prohibited include but are not limited to the following:

1. Any use that is illegal or in violation of other Board policies, including harassing, discriminatory or threatening communications and behavior, violations of copyright laws, etc.;

2. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive;
3. Any inappropriate communications with students or minors;
4. Any use for private financial gain, or commercial, advertising or solicitation purpose;
5. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school-sponsored organization; or to raise funds for any non-school-sponsored purpose, whether for profit or not-for-profit. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students, and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek guidance from the Director or other appropriate administrator;
6. Any communication that represents personal views as those of CFCI or that could be misinterpreted as such;
7. Downloading or uploading software or applications without permission from the appropriate administrator;
8. Opening of forwarding any e-mail attachment (executable files) from unknown sources and/or that may contain viruses;
9. Sending mass e-mails to school users or outside parties for school or non-school purposes without the permission of the appropriate administrator;
10. Any malicious use or disruption of CFCI computers, networks, and Internet services or breach of security features;
11. Any misuse or damage to CFCI computer equipment;
12. Misuse of the computer passwords or accounts (employees or other users);
13. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;
14. Any attempt to access unauthorized sites;
15. Failure to report a known breach of computer security to the appropriate administrator;
16. Using school computers, networks, and Internet services after such access had been denied or revoked; and
17. Any attempt to delete, erase or otherwise conceal any information stored on a school computer that violates these rules.

18. Use of CFCI equipment by any non staff member, with the exception of CFCI students who are engaged in appropriate CFCI school related activities.

D. No expectation of privacy

CFCI retains control, custody and supervision of all computers, networks and Internet services owned or leased by CFCI. CFCI reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school computers, including e-mail messaging and stored files.

E. Confidentiality of Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

F. Staff responsibilities to students

All staff are to monitor all student computer use. Students are not to use staff computers unless closely monitored by the staff member. The staff member is ultimately responsible for inappropriate use of their assigned computer.

G. Compensation for losses, cost and/or damages

The employee shall be responsible for any losses, cost or damages incurred by CFCI related to violations of this policy and/or these guidelines.

H. CFCI assumes no responsibility for unauthorized charges, cost or illegal use.

CFCI assumes no responsibility for any unauthorized charges made by employees including but not limited to credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or any illegal use of its computers such as copyright violations.

I. Employee acknowledgement required

Each employee authorized to access CFCI computers, networks and Internet services is required to sign an acknowledgment form stating that they have read this policy and these guidelines. The acknowledgment form will be retained in the employee's personnel file.

Approved 12-15-2009

812 Student Internet and Email Acceptable Use

Internet access and Electronic Mail (E-Mail) are now available to students and teachers in CFCI. We believe the Internet offers vast, diverse, and unique resources to both students and teachers. Our goal in providing this service is to promote educational excellence in school by facilitating resource sharing, innovation, and communication. To gain access to the Internet, all students under the age of 18 must obtain parental permission and must sign and return the User Agreement and Parent Permission Form.

Access to the Internet will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Families should be warned that some material accessible via the Internet could contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people.

While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages; but ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.

To that end, the CFCI supports and respects each family's right to decide whether or not to apply for access.

CFCI Internet and E-Mail Rules

Students are responsible for good behavior on school computer networks just as they are in a classroom or school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply.

The network is provided for students to conduct research and communicate with others. Access to network service is given to students who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege – not a right. Access entails responsibility.

Individual users of the CFCI computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with CFCI standards and will honor the agreements they have signed.

Network storage areas may be treated like school lockers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on CFCI servers would be private.

Within reason, freedom of speech and access to information will be honored. During school, teachers will guide students toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio, and other potentially offensive media.

Students are permitted to access personal email accounts only for appropriate school related activities. Teachers are to monitor any such access to insure compliance with this rule.

Disciplinary Action:

Individual users of the Internet are expected to abide by the generally accepted rules of network etiquette. The following are not permitted:

- **Accessing any sites with adult content and/or discussions**
- **Sending e-mail that is offensive and/or inappropriate (if you have any doubts, let your teacher read first)**
- **Using computers in any way to cause problems for others. For example, Writing that is hurtful to others; deleting, destroying or changing the work of others; and/or anything that an adult has warned you about.**

In the event a student engages in any of the above referenced activities, his/her access privileges will be revoked and other disciplinary measures may result.

Other deliberate misuse of internet privilege will result in the following consequences:

- Offense 1: warning and notification of parents
- Offense 2: temporary loss of internet privilege (not to exceed 30 calendar days)
- Offense 3: loss of privilege for the remainder of the year

Students will be financially responsible for any damages that they do to equipment, physically, or electronically.

Adoption

This Student Internet and Email Acceptable Use Policy was adopted by the Board of Directors at a public meeting, following normal public notice on September 20, 2016.

813 Copyright Compliance

The board recognizes and supports the limitations on unauthorized duplication and use of copyrighted materials. The board does not condone any infringement on the property rights of copyright owners. Employees, students and visitors are prohibited from the use or duplication of any copyright materials not allowed by copyright law, fair use guidelines sanctioned by Congress, licenses or contractual agreements. Willful or serious violations also are considered to be in violation of expected standards of behavior for employees and students and may result in disciplinary action in accordance with board policy.

Fair Use: Unless allowed as "fair use" under federal law, permission must be acquired from the copyright owner prior to copying copyrighted material. Fair use is based on the following standards:

- the purpose and character of the use;
- the nature of the copyrighted work;
- the amount of and the substantiality of the portion used; and
- the effect of the use upon the potential market for, or value or, the copyrighted work.

The Director or designee is responsible for providing information and training to personnel and students, as appropriate, to provide further guidance on the fair use of copyrighted materials, including in the following circumstances:

- single and multiple copying for instructional purposes;
- copying for performances and displays;
- off-air recording of copyrighted programs;
- use of "for home use only" videotapes;
- computer software
- copyrighted materials on the Internet and on-line data bases; and
- reproduction and loan of copyrighted materials by school media centers.

Approved 12-15-2009

814 Student Discipline and Liability

It is essential that computers and networks be protected from misuse and abuse by users so they can serve their instructional purpose. Engaging in behavior that damages communications equipment and/or programs or interferes with use of these resources by others will not be tolerated.

Unacceptable use includes, but is not limited to, the following:

1. Abusive or objectionable language
2. Malicious attempt to harm or destroy data of another user
3. Transmission of material in violation of any US or state regulation
4. Use for commercial purposes or political lobbying
5. Violation of Copyright laws
6. Plagiarism

More serious violations include

7. Deletion or alteration of any network files or configurations
8. Planting a virus on a network
9. Running software designed to access passwords
10. Perform any act, which leads to significant damage to network operations.

Students who are found to have committed any of the above violations or other prohibited computer related actions will be subject to consequences possibly including suspension of computer privileges and suspension from school. The teacher and Director or designee will confer to determine the specific circumstances and consequences on a case by case basis.

If abuse of computers, peripherals or networks causes damage, which is permanent or requires repair or replacement, the student will be liable for any charges and may be subject to criminal prosecution.

Approved 12-15-2009

816 Access To Services

The Cape Fear Center for Inquiry will comply with the procedures stated in the most current edition of Policies Governing Programs and Services for Children with Disabilities and with subsequent revision of such rules as adopted by the State Board of Education. Copies of the rules and regulations are on file in the Exceptional Children's Office.

Approved 12-15-2009

817 Remote Access Policy

Cape Fear Center for Inquiry's systems must be protected against unauthorized access, malicious access, and disruption of service. Authorized users may be permitted to remotely connect to web hosting systems and data repositories for the conduct of business only through secure, authenticated and carefully managed access methods.

Users of such systems should take every precaution to prevent compromising confidential data. Such precautions include using proper user IDs and passwords as well as securing of the actual device used for access. Devices used to access these systems should have the latest anti-virus software/definition files installed along with controls for ad-ware and spyware in place.

Approved 12-15-2009

818 Security Awareness Policy

Employees at the Cape Fear Center for Inquiry shall be aware of security issues when saving information on their computers and when backing up information to external media. Appropriate encryption technologies will be utilized when transferring confidential information.

Approved 12-15-2009

822 Virus Protection

The Instructional Technology Facilitator will ensure all computers have up to date anti-virus software installed. Automatic updates will be set to protect computers from new viruses. Training must take place to ensure that all computer users know and understand safe computing practices and perform frequent backups on sensitive data files.

Approved 12-15-2009

824 Network Security

In order to maintain network security, any CFCI server or network equipment will have appropriate firewall filtering appliance installed. This also includes any local area network gateway that provides Internet access. This appliance will provide an ICSA Labs certified firewall in which will be used to filter and restrict undesirable content from the student population.

Approved 12-15-2009

825 Internet Safety

It is the policy of CFCI to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

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.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the CFCI online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervising, Monitoring

It shall be the responsibility of all members of the CFCI staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of IT Specialist or designated representatives.

The Technology Teacher or designated representatives will provide age- appropriate training for students who use CFCI Internet facilities. The training provided will be designed to promote CFCI's commitment to:

a. The standards and acceptable use of Internet services as set forth in the CFCI Internet Safety Policy;

b. Student safety with regard to:

i. safety on the Internet;

ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and

iii. cyberbullying awareness and response.

c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of CFCI's acceptable use policies.

Other CFCI policies regarding Internet Safety are listed below:

-Policy 365 Educating Students About Online Behavior

-Policy 812 Student Internet and Email

-Policy 814 Student Discipline and Liability

-Policy 824 Network Security

APPROVED 11-21-2013

Adoption

This Internet Safety Policy was adopted by the Board of Directors at a public meeting, following normal public notice, on September 20, 2016.

826 Disaster Recovery Procedure

It is the responsibility of the computer user to back up their files in a responsible manner. If the computer stores mission critical information, the files should be backed up to an off site location. The computer user should back up other information at regular intervals.

If CFCI installs a network with a server, regular back up procedures will be established and followed. Procedures will specify back up responsibilities.

Approved 12-15-2009

840 Hardware and Software Procurement

Hardware

All hardware purchases must follow proper purchasing procedures and must be approved by the Director prior to purchasing. Purchasing of equipment that has not been approved by the Director may result in the equipment not being supported by the Instructional Technology Facilitator. All purchases must meet the minimum requirements.

Software

All software purchases must follow proper purchasing procedures and must be approved by the Director prior to purchase. Each year, the Instructional Technology Facilitator will outline supported software programs. Software that has not been pre-approved will not be supported or installed by the Instructional Technology Facilitator. All software should be inventoried and installed by the Instructional Technology Facilitator. No software is to be installed without prior approval from the Instructional Technology Facilitator.

Approved 12-15-2009

842 Equipment/Materials Donation

The Board of Directors recognizes the services of the CFCI Partnership, other organizations, and individuals in providing equipment for use in the schools and in upgrading existing facilities. Such services and donations should be made after conferences between the teacher, donor, and Director or designees, whose responsibility it is to see that such additions are in accord with administrative policies, particularly where installation costs are involved. All donations become school property.

Approved 12-15-2009

844 Inventory Control Policy

As part of the year-end procedures, the Technology Committee will perform an inventory of all computers and media equipment.

- The serial number, name and location of each piece of equipment are recorded in a database.
- Each year, the information in the database will be checked for accuracy. Any changes in location will be updated. The equipment will also be checked to make sure it is in operative condition.
- Any equipment unaccounted for will be reported to the Director.

Approved 12-15-2009

846 Equipment Maintenance and Repairs

The Technology committee will develop and implement a procedure for equipment maintenance and repair. This procedure will include a service request form to be completed if equipment needs to be serviced or repaired. Completed service request forms are to be collected by the Technology Committee for service history on the equipment.

Approved 12-15-2009