

<b>FREDERICK COUNTY PUBLIC SCHOOLS</b>		<b>Reg. No. 400-73</b>
<b>Subject:</b>	<b>COMPUTERS: ACCEPTABLE USE OF DIGITAL NETWORKS AND ONLINE RESOURCES</b>	<b>Date of Issue:</b> <b>4/1/96</b>
<b>Preparing Office:</b>	<b>Office of the Superintendent</b>	<b>Amended:</b> <b>6/3/09</b>

I. Policy

II. Procedures

A. Definitions (list is not intended to be all inclusive)

**1. Cyber Bullying**

Cyber bullying is an incident or a pattern of behavior that occurs through electronic mechanisms, which results in a person feeling intimidated or harassed by another. Cyber bullying behavior can impact the health/safety of students and/or be disruptive to the educational environment.

**2. Cyber Stalking**

Cyber stalking is the use of the Internet or other electronic means to stalk someone. This behavior includes false accusations, monitoring, the transmission of threats, identity theft, damage to data or equipment, the solicitation of minors for sexual purposes, and gathering information for harassment purposes.

**3. Cyber Threats**

Cyber threats include attacks from viruses, worms, trojan horses, phishing, denial of service (dos) attacks, unauthorized access (stealing intellectual property or confidential information), and control system attacks.

**4. Electronic Communication**

Any communication that is distributed on the Internet or World Wide Web (WWW) including e-mail, instant messaging, chat, blog posts, etc.

**5. Sexual Discrimination/Harassment**

Sexual harassment is a form of sexual discrimination and consists of unwelcome and unsolicited sexual advances, requests for sexual favors, sexually motivated physical conduct, or communication of a sexual nature by another person.

**6. Web 2.0/Read Write Web**

Web 2.0/Read Write Web are tools that enable students to publish content on the Internet. It is a collaborative place where people can interact. Some call it the participatory web. Students can not only read the web but write on it. Examples are blogs, wikis, podcasts, social networking, and other sites that allow students to post their work.

## B. Purpose

The purpose of this regulation is to establish guidelines for acceptable use of FCPS computer systems, the Internet, and the World Wide Web (WWW), hereafter referred to as digital networks and/or online resources.

Digital networks will be used to further the educational goals and objectives of the Frederick County Public Schools. Through electronic information and communication tools, an unprecedented, worldwide, diverse array of resources is now available in schools and classrooms to support and enrich the curriculum. Knowing how to access this wealth of information and how to communicate electronically will be fundamental skills in the world in which our students will be citizens and employees.

By facilitating resource sharing, innovation, and communication, digital networks promote educational excellence. Students are able to contribute to the collection, analysis, and dissemination of knowledge. Using resources on computer networks and the Internet can be an effective learning tool and motivator for students that encourages independent and critical thinking.

## C. Liability

1. FCPS will not guarantee the availability of access to network resources and will not be responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties.
2. The accuracy and quality of information obtained cannot be guaranteed, nor can information sent or received be assured to be private.
3. With worldwide access to computers comes the availability of material that may not be of educational value in the context of the school setting. FCPS cannot control or censor illegal, defamatory, inaccurate, or potentially offensive materials, which may be available to the user on systems accessible through FCPS.

## D. Digital Networks in Frederick County Public Schools

To emphasize that use of digital networks in the Frederick County Public Schools is for appropriate activities, this regulation requires that

1. Access will be provided for instructional use and school-related activities only.
2. Access will be provided via FCPS configured and/or approved network devices only.
3. Access will occur in the manner described below in Sections E., F., and G. that address responsibilities for all users, school staff and students.
4. FCPS complies with the implementation of the Children's Internet Protection Act (CIPA). Measures are taken to block or filter Internet access as required by CIPA.

5. Student Independent Internet Access

- a. Permits access to the Internet without adult supervision, except as noted below;
- b. Permits unsupervised access to electronic communication or other Internet messaging services for educational purposes with principal permission;
- c. Requires a completed Permission Form for Secondary Student Independent Access to the Internet (See attached Exhibit.); and
- d. Is permitted at the middle and high school levels and implemented in accordance with the terms of this regulation.

Note: At the elementary level, all Internet access must occur under the supervision of an adult approved by the school administration.

6. Directed Internet Use

- a. Requires appropriate adult supervision (i.e. staff members or their adult designees are present to the extent that adequate monitoring of student access to the Internet occurs);
- b. Is permitted at all levels and implemented in accordance with the terms of this regulation;
- c. Permits supervised access to electronic communication with principal approval; and
- d. Does not require a completed student independent access permission form.

7. Creation, Publication, and Maintenance of Student-Created Web Pages and Internet Sites

- a. All material created for and published on the web by students must comply with Regulation 400-77 – “Computers: FCPS Website Publishing.”
- b. Student-created web content associated with approved school activities may only be posted for public access after approval from the instructor, club advisor, and/or school administrator. All work will be accessible and editable by the supervising instructor who will be held responsible for monitoring online student material for appropriateness.
- c. Any private student-created web content that is created off school premises will not be considered FCPS responsibility unless it causes a substantial or material disruption to FCPS, its employees or students, or creates a matter of health and safety. This could include text, digital video, and/or audio depicting FCPS students, staff and property. Disciplinary consequences may be imposed in accordance with Regulation 400-8 – “Discipline.”

8. FCPS and its employees are not responsible for use that is in violation of this regulation. The school system reserves the right to review the content of all accounts. Network administrators may review files and communications to keep the network working properly and to ensure that users are using the system in accordance with FCPS regulations and applicable federal and state laws. Users should not expect that files or electronic communication messages would be private.

E. User Responsibilities for Students and Staff

1. Users are responsible for using the provided school account in an ethical, responsible and legal manner for school-related tasks only. Users will not jeopardize in any way the safety of students or staff of FCPS.
2. Using or importing offensive, obscene, libelous, disruptive, or inflammatory language, pictures, or other material on any computer or network within FCPS is prohibited.

Examples may include, but are not limited to:

- Bullying / Cyber Bullying
  - Denigration or Defaming Character
  - Offensive or Rude Messages
  - Gossips and Rumors that affect instruction
  - Cyber Stalking
  - Cyber Threats
  - Sexual Harassment
  - Comments that infer hate or bias based on race, religion, sexual orientation, or physical characteristics
3. If a user receives any harassing, threatening, or inappropriate material on the internet or digital network, the user should not respond and should immediately report the material to a teacher or the appropriate administrator.
  4. For safety reasons, users shall not label photographs posted online or reveal personal information such as home phone numbers or addresses except in specific circumstances where such information is required to complete academic assignments.
  5. Digital networks will be used for authorized activities only. Unauthorized activities include, but are not limited to: knowingly spreading viruses, worms, or any other malicious files, violating copyright laws (e.g. illegally sharing copyrighted material), installing or using unauthorized software, accessing the network via another user's account, unauthorized entry (hacking), advertising commercial products or services, mass unsolicited electronic mailings, and/or destruction of computer systems and files.
  6. Users will use the network in such a way that use of the network by other users is not intentionally disrupted.
  7. Users will not circumvent or disable filtering or other technology protection measures put in place by system administrators, without proper authorization.
  8. Files and electronic communication messages, or posts of any kind created or stored on equipment or media covered under this regulation are the property of the Frederick County Public Schools, and can be used as evidence in a court of law.

9. Users will not divulge their passwords to, or otherwise allow access to their network accounts by, anyone other than authorized supervisors for the purpose of maintaining the network or implementing this regulation.
10. Users will use all resources on digital networks in accordance with the policies of the institutions providing the service and the procedures developed by FCPS.

F. Additional Staff Responsibilities

1. Access to digital networks on FCPS equipment by staff members is governed by Regulation 300-45, "Computers - Staff Use."
2. Staff will model safe and appropriate use of digital networks for students per the expectations set in this policy.
3. Staff members assigning directed Internet use will pre-screen network resources in order to specify those which are applicable to the curricular needs of the assignment and the developmental level of the student(s).
4. Staff members assigning an independent Internet activity will assure that such activities and available resources are applicable to the curricular needs of the assignment and the developmental level of the student(s), and that signed permission forms for student independent access are on file for all students participating in the activity.
5. Just as in any classroom situation, the teacher is responsible for providing appropriate adult supervision and monitoring of the learning activities.
6. In schools where independent Internet activities are allowed, each school will provide for the distribution, collection, and monitoring of the permission forms for student independent access.
7. Staff members assigning or permitting use of digital networks will ensure that instruction in acceptable use of digital networks has occurred. Topics to be taught include:
  - a. Content of Regulation 400-73 – "Computers: Acceptable Use of Digital Networks and Online Resources"
  - b. Procedure for accessing appropriate network resources
  - c. Procedures for using specific Internet tools
  - d. Using the generally accepted rules of network etiquette as outlined in Section G. "Additional Student Responsibilities" and on the Student Independent Access to the Internet permission form
  - e. Copyright issues
  - f. Privacy issues
  - g. Safety guidelines on the Internet
  - h. Respect for time and resource use

- i. Acquiring skills needed to make judgments about locating and using information, which matches the learner's instructional level and the learning objectives of the assignment
- j. Discriminating among types of information sources, and assessing the appropriateness of using the Internet as a resource for a specific learning activity
- k. Applying the same criticism of educational accuracy and suitability used for all educational resources

G. Additional Student Responsibilities

- 1. Students are responsible for their behavior on school computer networks.
- 2. Students will access only those network resources for which they have obtained permission, using the account assigned to them.
- 3. Students will use appropriate language and follow the same code of conduct as required by FCPS and individual school building policies. Students will communicate only in a respectful and appropriate manner.
- 4. Students in all middle and high schools may have independent access to the Internet. Parent permission is required and both the student and the parent or guardian must sign the student independent access permission form. By signing this form, the student agrees to act in a considerate and responsible manner.
- 5. Students may not install software on FCPS equipment unless instructionally directed to do so.

H. Consequences of Violations

Equipment found to contain unauthorized files (such as illegal copies of software, evidence of access to inappropriate web addresses, unauthorized encryption software, electronic communication, and student-created content in violation of policy or regulation, etc.) will serve as evidence in disciplinary action.

Violations of this regulation will subject the violator to disciplinary action in accordance with Frederick County Public School disciplinary policies and may include loss of access to resources covered under this regulation, and/or criminal sanctions. In addition, any illegal activities will be reported to the appropriate agencies.

Approved:

*original signed by*

---

Linda D. Burgee  
Superintendent

**EXHIBIT**

**FREDERICK COUNTY PUBLIC SCHOOLS  
PERMISSION FORM FOR SECONDARY STUDENT  
INDEPENDENT ACCESS TO THE INTERNET\***

**Parent/Guardian Permission**

I  agree to the following  do not agree to the following:

As the parent or legal guardian of the minor student signing below, I grant permission for my son or daughter to have independent access to services such as the Internet and electronic mail. I understand that:

- He/she will be taught the provisions of the Computers: Digital Networks Acceptable Use regulation of Frederick County Public Schools prior to using digital networks.
- Individual students will be held liable for violations.
- Some materials on the Internet may be objectionable, including:
  - Images and text of an illegal, defamatory, inaccurate, or potentially offensive nature
  - Unmonitored chat rooms
  - Inappropriate World Wide Web sites

*Note: Although accessing objectionable material is prohibited by the Computers: Digital Networks Acceptable Use regulation, a student may find ways to do so.*

I accept responsibility for setting and conveying standards for my son or daughter to follow when selecting, sharing or exploring information and media.

Parent/Guardian Signature \_\_\_\_\_ Date \_\_\_\_\_

Parent/Guardian Name (please print) \_\_\_\_\_

**Student Information:**

Name \_\_\_\_\_

School \_\_\_\_\_

Grade \_\_\_\_\_ Graduation year \_\_\_\_\_ Birth Date \_\_\_\_\_

Street Address \_\_\_\_\_ Home Telephone \_\_\_\_\_

**Student User Agreement**

I hereby agree to abide by the rules stated in the Computers: Digital Networks Acceptable Use regulation of Frederick County Public Schools, and to comply with all relevant laws, restrictions, and regulations while communicating over the network.

Student Signature \_\_\_\_\_ Date \_\_\_\_\_

\* Permits access to Internet services without adult supervision. Messaging services, such as electronic communication or chat, require the permission of the principal.