Regulation 6410.9
Information Technology
Information Technology
Operations
Effective 04-14-08

INFORMATION TECHNOLOGY

Technology Infrastructure

Appropriate Use of Fairfax County Public Schools' Network and Internet Resources

This regulation supersedes Regulation 6410.8.

I. PURPOSE

To provide requirements and assign responsibilities that are consistent with Fairfax County Public Schools (FCPS) educational objectives and security requirements for the use of Internet resources and network services by FCPS. This regulation covers all users of FCPS network services.

II. SUMMARY OF CHANGES SINCE LAST PUBLICATION

A. Section IV.H. has been revised to increase the number of broadcast e-mail messages allowed to be sent to FCPS employees from outside the network within a 12-hour period from 500 to no more than 2,000. Also, a sentence has been added to clarify that there is an existing size limit of 4 MB for incoming messages.

B. Section V.S. has been revised to update the department and job title of the person responsible for official information posted on the web.

C. Section VI.D. has been revised to increase the number of broadcast e-mail messages allowed to be sent to FCPS employees from outside the network within a 12-hour period from 500 to no more than 2,000.

III. SCOPE

A. Applicability

This regulation applies to all users of FCPS network services and computer systems and to all students and staff members when representing FCPS, regardless of the computer system used.

B. Definitions

1. Acceptable Use Policy (AUP)

A contract signed by parents and students — or guidelines for FCPS staff members and contractors — that sets the rules for using the FCPS network.

2. Browser

   A program that runs on a computer and allows a user to access web pages available on the World Wide Web (WWW). *Netscape Navigator* or *Communicato*r and *Microsoft Internet Explorer* are examples of browser software.

3. Child Pornography

   Sexually explicit visual material using or having as a subject a person less than 18 years of age. (Code of Virginia, section 18.2-374.1:1)

4. Core System

   A mission-critical application or system that is protected from general public access.

5. Firewall

   A combination of software and hardware that makes it possible for an organization to block inbound and outbound traffic on a network.

6. Harmful to Juveniles

   Quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

   a. predominantly appeals to the prurient, shameful, or morbid interest of juveniles.

   b. is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for juveniles.

   c. is, when taken as a whole, lacking in serious literary, artistic, political, or scientific value for juveniles. (Code of Virginia, section 18.2-390)

7. Inappropriate Content

   Content known to be obscene, to be harmful to juveniles, or to be child pornography (Code of Virginia, section 18.2-374.1:1) and content known to promote, encourage, or provide the skills to commit illegal activities. (See the current version of Policy 6401.)

8. Information Systems

   Includes, but is not limited to, hardware, software, communication lines and devices, terminals, printers, CD-ROM devices, tape drives and servers, and mainframe and personal computers.

9. Internet Access

Includes all methodologies used to connect to Internet servers and users around the world and all methods for providing access regardless of funding or facilitating sources.

10. Internet Service Provider

    The commercial vendor that FCPS uses on a contractual basis to provide the interface and/or connectivity between the FCPS wide-area network (WAN) and the Internet.

11. Internet Services

    Includes access to external systems and information sources using the Internet, access to and hosting of WWW services and information, and use of Internet tools such as FTP, gopher, Telnet, chat, e-mail, etc.

12. Obscene

    Describes that which, considered as a whole, has as its dominant theme or purpose an appeal to the prurient interest in sex, that is, a shameful or morbid interest in nudity, sexual conduct, sexual excitement, excretory functions or products thereof, or sadomasochistic abuse, and which goes substantially beyond customary limits of candor in description or representation of such matters and which, taken as a whole, does not have serious literary, artistic, political, or scientific value. (Code of Virginia, section 18.2-372)

13. System Administrator

    An individual responsible for managing accounts, applications, and system software on an FCPS server or workstation.

14. Users

    All staff members, students, volunteers, parents, employee organizations, and other individuals when they are using FCPS network and Internet resources.

15. Web Page

    A page of information located on a web server and accessible through the Internet. The page can contain a mixture of graphics and text and can include hyperlinks to other such pages.

16. Web Server

    A program that runs on any computer, large or small, that responds to requests for documents (web pages and downloadable files) sent to it by a web browser or an FTP client.

17. World Wide Web (WWW)

    A graphical interface to most Internet resources.

IV. REQUIREMENTS

A. The principal or program manager shall approve all FCPS access to Internet resources and to FCPS computer systems.

B. User access to FCPS core systems shall require the permission of the designated system administrator. Access by non-FCPS users to core systems shall require the approval of the FCPS chief information officer.

C. All users are prohibited from knowingly accessing portions of the Internet that do not promote the educational or instructional mission or administrative function of FCPS.

D. Students are prohibited from knowingly accessing inappropriate Internet content.

E. All users are prohibited from using computers or the FCPS network to commit, facilitate, encourage, or promote illegal acts.

F. All users are prohibited from using computers or the FCPS network to commit, facilitate, encourage, or promote the unauthorized or fraudulent use of a credit card.

G. E-mail access, if provided, shall comply with all FCPS policies and regulations including, but not limited to, privacy, standards of conduct, and the use of FCPS equipment. FCPS may review e-mail sent by FCPS users to verify compliance with FCPS policies and regulations.

H. All users are prohibited from using computers or the FCPS network to forge or interfere with electronic mail messages. Broadcast e-mail messages transmitted from outside the FCPS network to FCPS users should be limited to no more than 2,000 recipients within a 12-hour period. Any incoming e-mail messages cannot exceed the current existing limit of 4 MB.

I. The use of computer systems for personal use unrelated to the mission of FCPS or for private gain should be kept to a minimum. Note: Staff development activities are considered to be “mission-related.”

J. All users are prohibited from using the FCPS network to market commercial products and services.

K. All users are prohibited from using computers or the FCPS network to harass or threaten individuals or groups. Any organization sending unsolicited broadcast e-mail messages to users on the FCPS network will be filtered from sending future e-mail messages.

L. All users are prohibited from vandalizing computers or the FCPS network. This is to include attempts to alter or destroy data of another user or to endanger the integrity of a computer or the FCPS network or the data stored thereon (including the

introduction of any virus, time bomb, trojan horse, or the like), any deletion of or alteration to system files or data, and any damage to equipment. The unauthorized examination or copying of files or data belonging to others is also defined as vandalism.

M. Introduction of any virus, time bomb, trojan horse, or the like), any deletion of or alteration to system files or data, and any damage to equipment. The unauthorized examination or copying of files or data belonging to others is also defined as vandalism.

N. Outbound access to the Internet shall be in accordance with applicable FCPS rules and regulations. Monitoring and management of acceptable use are the responsibility of the principal or program manager.

O. Schools shall require that all students and parents sign the acceptable use policy document (Attachment A) and retain a copy of the signed document in the main office. FCPS employees and contractors shall read and comply with guidelines in Attachment B.

P. Inbound access to FCPS systems and services from the Internet shall be restricted to the FCPS network segment outside the firewall unless otherwise authorized by the chief information officer. (This includes Internet services such as HTTP [web], FTP, Telnet, time, gopher, ping, finger, etc.)

Q. All changes to the FCPS firewall configuration must be approved in advance by the FCPS chief information officer or his or her designee.

R. Users shall not reveal their passwords to anyone. Users are prohibited from using passwords or accounts other than their own.

S. Copyrighted materials shall not be downloaded from the Internet or further transmitted in any form without compliance with all terms of a preauthorized agreement. FCPS will not tolerate infringement or violation of United States or international copyright laws or restrictions.

T. All users are prohibited from using computers or the FCPS network to publish any text, image, or sound that contains content that is obscene or harmful to juveniles; that promotes, encourages, or provides the skills to commit illegal, criminal activities; or that is child pornography.

V. RESPONSIBILITIES

A. The FCPS chief information officer shall provide and administer FCPS Internet services, Internet protocol (IP) addresses, and connectivity between the FCPS network infrastructure and the Internet service provider and shall manage the FCPS central web servers.

B. The FCPS chief information officer may direct system administrators to impose limitations on the retention, volume, and size of messages and data (including e-mail) transmitted and stored on FCPS network resources to ensure the integrity of the network and maximize data flow for all users.

C. The FCPS chief information officer may regulate the management and the proper use of information system resources in the form of technical bulletins.

D. Users are responsible for complying with FCPS rules, regulations, and "acceptable use policies."

E. Central offices will provide information for school staff members and parents to promote a consistent and accurate understanding regarding appropriate use of network resources.

F. Central offices will educate staff members on personal safety practices and effective techniques for identifying and evaluating information and its sources.

G. Schools will educate students on personal safety practices and effective techniques for identifying and evaluating information and its sources.

H. Directors of instructional department offices are authorized to approve Internet blocking categories for their respective schools, centers, and academies in conformance with the current version of Policy 6401 and in accordance with procedures in the current version of Regulation 3005.

I. The school principal or his or her designee is authorized to approve changes to Internet blocking lists to include adding or removing web site addresses (URLs) deemed to be inappropriate or appropriate material in accordance with procedures in the current version of Regulation 3005.

J. School principals or their designees will handle challenges regarding blocking of individual Internet sites in accordance with the current version of Regulation 3009.

K. Directors of instructional department offices will handle challenges to categories of Internet sites in accordance with procedures in the current version of Regulation 3009.

L. Schools will review the acceptable use policy with students and enforce rules of conduct necessary to foster appropriate student use of network resources.

M. Schools will establish expectations for student behavior when encountering inappropriate material.

N. School staff members will practice classroom management and monitoring techniques, to the extent feasible, to encourage appropriate use of network resources.

O. The Department of Special Services (SS) and the Instructional Services Department (IS) will integrate responsible use of network resources and technology into appropriate curricula.

P. SS, IS, and the Department of Information Technology (IT) will identify recommended Internet resources and sites that support the curriculum in accordance with the current version of Regulation 3005.

Q. Schools and the Hearings office will implement and monitor processes to inhibit, to the extent feasible, student access via network resources to contents known to:

1. be obscene.

2. be harmful to juveniles.

3. be child pornography.

4. promote, encourage, or provide the skills to commit illegal activities (see the current version of Regulation 2601).

R. SS, IS, and IT will develop instructional and technological strategies for schools to provide students with reasonable protection from inappropriate Internet content.

S. Principals and program managers are responsible for the accuracy and appropriateness of materials posted on school or department web pages and for ensuring that the materials are consistent with official information posted by the assistant superintendent, Department of Communications and Community Outreach.

T. If any FCPS employee, student, or network user becomes aware of inappropriate use of network resources, the person is expected to bring it to the attention of a responsible teacher, principal, or program manager, who will determine if any applicable policy or regulation has been violated and take the appropriate action.

VI. EMPLOYEE ORGANIZATION USE OF ELECTRONIC MAIL (E-MAIL)

An employee organization may use the FCPS e-mail system to send information that is related to the school system in accordance with the following guidelines:

A. To obtain an FCPS e-mail account, the organization shall:

1. be certified under the School Board's registration procedure.

2. each year submit a written request to the chief information officer for account creation or renewal.

B. The organization must comply with the requirements stated in section III. of this regulation.

C. E-mail communications transmitted via the FCPS e-mail system shall be identified as to their senders.

D. Use of e-mail conferences or folders is encouraged to reach a broader audience. Broadcast e-mail messages transmitted from outside the FCPS network to FCPS employees should be limited to no more than 2,000 recipients within a 12-hour period.

E. Use of e-mail to solicit nonmembers of the organization to become members is not permitted.

F. Use of e-mail for mass mailings to nonmembers is prohibited.

G. Use of e-mail to endorse or oppose a candidate for public office is not permitted.

H. Any employee organization found in violation of these guidelines shall receive written notification of termination of its e-mail account. An employee organization shall have 14 days from receipt of such notice to show why such termination should not take place.

VII. INTERNET SAFETY

A. This Fairfax County Public Schools (FCPS) regulation, in conjunction with the companion FCPS Internet safety web sites http://fcpsnet.fcps.edu/is/oiti/InternetSafety/ and http://www.fcps.edu/dis/OITI/InternetSafety/, defines the Internet safety program criteria as required by Title § 22.1-70.2 (v) of the *Code of Virginia,* which specifies that each school division implement an Internet safety program that is integrated within the division's instructional program. These links are available only on computer within the FCPS system.

B. The Internet safety program described on the companion web sites shall follow a review and revision cycle at a minimum of every two years.

VIII. ATTACHMENTS

Acceptable use policies for schools, centers, and offices are attached for use by principals and program managers.

Legal References: Code of Virginia, sections 18.2-372, 18.2-374.1:1, and 18.2-390

See also the current versions of: Regulation 1505, Management of Fairfax County Public Schools' Internet Presence
Regulation 2601, Student Responsibilities and Rights Booklet
Regulation 2610P, Removal (Suspension, Expulsion, or Exclusion) of Students From School
Regulation 3005, Program and Supplemental Instructional Print Materials Identification, Evaluation, and Approval
Regulation 3009, Challenged Library and Instructional Materials
Policy 6401, Student Use of FCPS Network and Internet Resources
Regulation 6801, School Library Media Centers

Attachments

Acceptable Use Policy for Student Network Access

The information systems and Internet access available through FCPS are available to support learning, enhance instruction, and support school system business practices.

FCPS information systems are operated for the mutual benefit of all users. The use of the FCPS network is a privilege, not a right. Users should not do, or attempt to do, anything that might disrupt the operation of the network or equipment and/or interfere with the learning of other students or work of other FCPS employees. The FCPS network is connected to the Internet, a network of networks, which enables people to interact with millions of networks and computers.

All access to the FCPS network shall be preapproved by the principal or program manager. The school or office may restrict or terminate any user's access, without prior notice, if such action is deemed necessary to maintain computing availability and security for other users of the systems. Other disciplinary action may be imposed as stated in the Fairfax County Public Schools Student Responsibilities and Rights (SR&R) document.

FCPS implements Internet filtering on all FCPS sites in accordance with the federal Children's Internet Protection Act. Schools will continually educate students on personal safety practices and effective techniques for identifying and evaluating information and its sources.

Respect for Others

Users should respect the rights of others using the FCPS network by:

- Using assigned workstations as directed by the teacher.
- Being considerate when using scarce resources.
- Always logging off workstations after finishing work.
- Not deliberately attempting to disrupt system performance or interfere with the work of other users.
- Leaving equipment and room in good condition for the next user or class.

Ethical Conduct for Users

Accounts on the FCPS network, both school-based and central, are considered private, although absolute security of any data cannot be guaranteed. It is the responsibility of the user to:

- Use only his or her account or password. It is a violation to give access to an account to any other user.
- Recognize and honor the intellectual property of others; comply with legal restrictions regarding plagiarism and the use and citation of information resources.
- Not read, modify, or remove files owned by other users.
- Restrict the use of the FCPS network and resources to the mission or function of the school system. The use of the FCPS network for personal use or for private gain is prohibited.
- Help maintain the integrity of the school information system. Deliberate tampering or experimentation is not allowed; this includes the use of FCPS network and resources to illicitly access, tamper with, or experiment with systems outside FCPS.
- Refrain from using offensive, obscene, or harassing language when using FCPS network systems.
- Abstain from accessing, changing, or deleting files belonging to others.

Respect for Property

The only software, other than students' projects, to be used on school computers or the school network are those products that the school may legally use. Copying copyrighted software without full compliance with terms

of a preauthorized license agreement is a serious federal offense and will not be tolerated. Modifying any copyrighted software or borrowing software is not permitted.

- Do not modify or rearrange keyboards, individual key caps, monitors, printers, or any other peripheral equipment.
- Report equipment problems immediately to teacher or program manager.
- Leave workstations and peripherals in their designated places.

Internet Safety and Security

- Information may not be posted if it: violates the privacy of others, jeopardizes the health and safety of students, is obscene or libelous, causes disruption of school activities, plagiarizes the work of others, is a commercial advertisement, or is not approved by the principal or program manager.
- Users will not change or delete files belonging to others.
- Real-time messaging and online chat may only be used with the permission of the teacher or program manager.
- Students are not to reveal personal information (last name, home address, phone number) in correspondence with unknown parties.
- Users exercising their privilege to use the Internet as an educational resource shall accept the responsibility for all material they seek.
- Users are responsible for reporting any inappropriate material they receive.
- Users are prohibited from accessing portions of the Internet that do not promote the instructional mission of FCPS.
- All student-produced web pages are subject to approval and ongoing review by responsible teachers and/or principals. All web pages should reflect the mission and character of the school.
- Users are prohibited from viewing, sending, and accessing illegal material.
- Students have the responsibility to cite and credit all Internet material used.
- Students are prohibited from downloading inappropriate or illegal material on FCPS computers.

Related Documents: The current versions of Regulation 6410, Appropriate Use of Fairfax County Public Schools' Network and Internet Resources, and Regulation 2601, Student Responsibilities and Rights.

Acceptable Use Policy for Staff Member and Contractor Computer Systems and Network Access

The information systems and Internet access available through FCPS are available to support learning, enhance instruction, and support school system business practices.

Employees and contractors should read and comply with FCPS policies and regulations regarding use of FCPS information systems including: the *Employee E-Mail Handbook* and the current versions of Regulations 1505, 4293, 4429, 6220, 6222, and 6410.

FCPS information systems are operated for support of the educational mission of the school system. The use of the FCPS network is a privilege, not a right. Users should not do, or attempt to do, anything that might disrupt the operation of the network or equipment, interfere with the learning of students, or impair the work of other FCPS employees.

The FCPS network is connected to the Internet, a network of networks, which enables people to interact with millions of networks and computers. The principal or program manager determines who may have access to the FCPS network, and he or she may restrict or terminate any user's access, without prior notice, if such action is deemed necessary to maintain computing availability, ensure appropriate use, or protect security. The principal or program manager may discipline any individual who violates this policy or school system regulations regarding the network.

Property Ownership

FCPS computers, systems, and network resources are the property of the school system. They may not be altered in any way, unless authorized by a school-based technology specialist (SBTS), technology support specialist (TSSpec), or program manager. Any work prepared on or with the assistance of FCPS information systems or network resources is the property of FCPS. It cannot be licensed or sold for the benefit of any individual employee or user.

Software instructions and license agreement terms must be strictly followed. Duplicating copyrighted software, without fully complying with license agreement terms, is a serious federal offense and will not be tolerated. Having a copy of a piece of software does not constitute authorization for modifications or additional copies of the software to be made; most licenses prohibit such uses. Installing unlicensed software is not permitted. Users should:

- Check with an SBTS or a TSSpec on software license agreement terms.
- Not install personal software on school system equipment unless authorized by an SBTS, a TSSpec, or a program manager.
- Contact an SBTS or a TSSpec for assistance with modifying, removing, or rearranging keyboards, individual key caps, monitors, printers, or any other peripheral equipment.
- Report equipment problems immediately to an SBTS, a TSSpec, or a program manager.

Respect for Others

Respect the rights of others using the FCPS computers and network by:

- Using assigned workstations as directed.
- Being considerate when using scarce resources.
- Always logging off workstations after finishing work.
- Not disrupting system performance or interfering with the work of other users.
- Leaving equipment and room in good condition for the next user or class.

Ethical Conduct and Appropriate Use

Users should observe the following rules:

- Use FCPS systems and network resources for school system business. Keep personal use of such resources to a minimum.
- Only use assigned accounts or passwords. Do not provide passwords to anyone unless directed by an SBTS, a TSSpec, or a program manager. Never share an account or password with students or those outside the school system. If a password must be shared with another employee because of an emergency, notify an SBTS or a TSSpec, and change the password within 24 hours.
- Recognize and honor the intellectual property of others. Do not plagiarize. Comply with legal restrictions regarding the use and citation of others' work.
- Do not read, modify, disclose, or remove files owned by other users without their permission or the authorization of an SBTS, a TSSpec, or a program manager.
- Do not use the FCPS network or resources illegally to access, tamper with, or experiment with systems outside FCPS.
- Do not use offensive, obscene, libelous, or harassing language when using any FCPS network system.
- Do not post or send information that violates the privacy of others, jeopardizes the health and safety of others, disrupts school or office activities, or is inconsistent with the school system's mission. Remember that anything sent or posted on a school system computer is identifiable as originating from FCPS and reflects on the school system.
- Use real-time messaging and online chat only with the permission of a principal or a program manager and only for school system business.
- Users are responsible for all material maintained on their systems and in their accounts. If inappropriate or unsolicited material is received, it should be deleted immediately. If it is repeatedly received and cannot be stopped, contact an SBTS or a TSSpec for assistance.
- Do not use FCPS networks or systems to access portions of the Internet that do not promote the instructional mission of FCPS.
- All web pages should reflect the mission and character of the school system. Creation of web pages should be in compliance with Regulation 1505 and with the approval of a principal or a program manager.
- *E-mail is not confidential or private; it is the property of the school system.* FCPS may review all e-mail sent or received by employees, including deleted messages. E-mail should be used primarily for FCPS business; personal use should be incidental and minimal. E-mail may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-FCPS purposes. "Spamming" is prohibited by law as well as by FCPS policy.
- E-mail messages should be professional and relate to FCPS business. E-mail signatures may include name, title, addresses, phone, and fax numbers. School or department mottos may also be included. Please refrain from including other slogans or sayings in the signature portion of your e-mail messages.