Regulation 6410.17
Information Technology
Office of Cybersecurity

INFORMATION TECHNOLOGY

Technology Infrastructure

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

This regulation supersedes Regulation 6410.16.

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 FCPS technology resources. This regulation covers all use of FCPS technology resources, networks, and services on-premises and off-premises.

II. SUMMARY OF CHANGES SINCE LAST PUBLICATION

A. Section I adds coverage of all FCPS technology resources, networks, and services on-premises and off-premises.
B. Section III adds a definition for Need-To-Know Principle, Confidential Data, Sensitive Data, and Private Data, and Parent.
C. Section III.I updates inappropriate content to include threatening and harassing content.
D. Section III.F adds tablets, licensed software, Software as a Service, and Hosted applications as examples of FCPS Technology Resources.
E. Section III.T adds contractors as a user type.
F. Section V adds the role of the DIT Office of Cybersecurity (OCS).
G. Section X adds additional user responsibility and prohibited uses of technology resources.
H. Section XII.B.7 adds reporting requirements for trademark infringement and entities fraudulently impersonating FCPS.
I. Attachment A requires adult supervision for students under five years of age when using FCPS technologies.
J. Attachment A defines students' ability to capture photographs or video during school hours, or on school property.
K. Attachment A prohibits the use of phones, tablets, and other mobile devices in restrooms and locker rooms.
L. Attachment A defines the access to social media for students.
M. Attachment A adds responsibility to ensure that use of student assigned devices is limited to supporting the educational outcomes of the student and the device not be used by anyone else for non-educational purposes.
N. Attachments A and B grant account access to only currently enrolled students and employees

III. DEFINITIONS

A. Acceptable Use Policy (AUP) Regulation

A document that establishes the rules for everyone who uses FCPS technology resources. The FCPS AUP is set forth in this regulation and attachments.

B. Browser

A program that runs on a computer allows users to access web pages available on the World Wide Web (WWW). Google Chrome is an example of browser software.

C. Child Pornography

Sexually explicit visual material using or having as a subject a person less than 18 years of age, as defined in the Code of Virginia, Section 18.2-374.1.

D. Core System

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

E. Confidential Data

Information that should only be seen by staff who require this information for official FCPS tasks.

Access to confidential information is based on the "need-to-know" principle that a recipient must require access to, knowledge of, or possession of the information to perform their job.

F. FCPS Technology Resources

Any information technologies issued or maintained by FCPS, including but not limited to, the FCPS network and network devices, servers, personal computers (PC), tablets, laptops, mobile phones, handheld devices, licensed software, Software as a Service, hosted applications, smartboards, printers, projectors, phones, and/or voicemail systems.

G. Firewall

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

H. **Harmful to Juveniles**

As defined in the Code of Virginia, Section 18.2-390, that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, and/or sadomasochistic abuse, when it:

Predominantly appeals to the prurient, shameful, and/or morbid interest of juveniles.

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

Is taken as a whole, lacking in serious literary, artistic, political, and/or scientific value for juveniles.

I. **Inappropriate Content**

As defined in the Code of Virginia, Section 18.2-374.1, content known to be obscene, to be harmful to juveniles, or to be child pornography, content known to promote, encourage, and/or to provide the skills to commit illegal activities, and content of a threatening or harassing nature.

J. **Information Systems**

A collection of hardware, software, services, people, and processes that collects, filters, processes, creates, distributes, and maintains data, provides computing and networking services.

K. **Internet Access**

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

L. **Internet Service Provider**

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

M. **Internet Services**

Includes access to external systems and information sources using the internet, access to and hosting of services and information, and/or the use of internet tools.

N. **Need-To-Know Principle**

Sharing information with recipients that require access to, knowledge of, or possession of the information to perform tasks or services essential to carry out official duties.

O. **Obscene**

As defined in the Code of Virginia, Section 18.2-372, 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, and/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, and/or scientific value.

P. **Parent**

Any parent, guardian, legal custodian, or other person having control or charge of a child.

Q. **Private Data**

Information regarding an individual, or a group of employees. This can contain but is not limited to Personally Identifiable Information (PII) or Protected Health Information (PHI).

R. **Sensitive Data**

Sensitive data includes protected/internal, private, and confidential data

S. **System Administrator**

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

T. **Users**

All staff members, contractors, students, volunteers, parents, guests, and all other individuals when they are using FCPS computing and networking resources or FCPS information systems.

U. **Web Page**

A page of information located on a web server and accessible through the internet.

V. **Web Server**

A program that runs on any computer, large or small, that responds to requests for contents or services sent to it by a web browser or client software.

W. **WWW**

A network of online content that can be accessed over the internet.

IV. ROLE OF ASSISTANT SUPERINTENDENT

A. The Assistant Superintendent, Department of Information Technology (DIT), is responsible for the planning, budgeting, security, and performance of FCPS information systems. The assistant superintendent, DIT, shall direct the development and implementation of the information system, assign roles, delegate responsibilities, and advise the School Board and leadership team (LT) members on information systems and information technologies.

B. The assistant superintendent, DIT, may regulate the management of the information systems and the proper use of technology resources in the form of regulations and technical bulletins

V. ROLE OF DIT-Office of Cybersecurity (OCS)

A. OCS is responsible for assessing security risk and approving software, hardware, vendors and services.

B. OCS is responsible for creating and enforcing data storage and security guidelines, policies, procedures, and protocols.

C. OCS is responsible for determining and overseeing the implementation of appropriate cybersecurity controls on FCPS devices, systems, services, and accounts.

VI. APPROVAL FOR USE OF FCPS TECHNOLOGY RESOURCES

A. The principal or program manager shall approve all user access to FCPS technology resources.

B. Access to FCPS core systems by an FCPS user shall require the permission of the designated system administrator. Access by non-FCPS users to core systems shall require the approval of the FCPS assistant superintendent, DIT.

C. All users must adhere to FCPS AUP, the rules set forth by this regulation and its attachments, as well as all other FCPS policies and regulations.

VII. INTERNET SAFETY PROGRAM

A. This regulation, in conjunction with the companion FCPS internet safety websites, https://sites.google.com/fcpsschools.net/fcpsdigcit/home (FCPS credential required) and https://www.fcps.edu/resources/technology/technology-literacy/digital-citizenship, define the internet safety program criteria as required by Virginia, which requires that each school division implement an internet safety program that is integrated within the division’s instructional program.

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

VIII. INTERNET SAFETY INSTRUCTION FOR STUDENTS

A. The departments of Special Services (DSS) and Instructional Services (IS) will integrate internet safety and the responsible use of technology resources into appropriate curricula, including personal safety practices and effective techniques for identifying and evaluating information and its sources.

B. DSS, IS, and DIT will identify recommended internet resources and sites that support the curriculum in accordance with the current version of Regulation 3005, Program and Supplemental Instructional Print Materials Identification, Evaluation, and Approval.

C. DSS, IS, and DIT will develop instructional and technological strategies for schools to provide students with reasonable protection from inappropriate internet content.

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

E. In addition to implementing the curricula referenced in Section VII.A., school staff members will practice classroom management and monitoring techniques, to the extent feasible, to encourage appropriate use of technology resources.

IX. INTERNET FILTERS AND BLOCKING

A. FCPS uses technology protection measures to block or filter access, as much as reasonably possible, to visual and written depictions that are obscene, pornographic, and/or harmful to minors over the network.

B. Directors of IS department offices are authorized to approve internet blocking categories for their respective schools, centers, and/or academies in conformance with the current version of Policy 6401, Use of FCPS Network and Internet Resources, and this regulation; and in accordance with Regulation 3005.

C. School principals and/or designees are authorized to request changes to internet blocking lists to include adding or removing website addresses (URLs) deemed to be inappropriate or adding appropriate material in accordance with procedures in Regulation 3005. Websites or categories deemed unsafe by the Office of Cybersecurity (OCS) shall not be approved.

D. Students, parents, and community members who believe that a website address has been inappropriately blocked or allowed should direct their concern to the following:

1. Directors of IS offices will handle challenges to categories of internet sites in accordance with procedures in Regulation 3009, Challenged Library and Instructional Materials.

2. School principals and/or their designees will handle challenges regarding blocking of individual internet sites in accordance with all procedures in Regulation 3009.

X. USER RESPONSIBILITIES AND PROHIBITED USES

A. Users are responsible for complying with FCPS rules, policies, and regulations; including this regulation, and any additional terms set forth in the applicable attachments.

B. Users are prohibited from tampering with FCPS technologies and attempting to circumvent security policies and controls enforced by the Office of Cybersecurity (OCS), such as, but not limited to, accessing the internet via proxy or unauthorized VPN services, logging on as an administrator to FCPS devices.

C. Users are responsible for complying with all data security guidelines set forth by the Office of Cybersecurity (OCS), such as, but not limited to, practicing the need-to-know principle and encrypting all emails that contain sensitive, private, or confidential information.

Written approval from OCS is required before the bulk exchanging of sensitive, private, or confidential information outside FCPS, such as, but not limited to, vendors and partner organizations. Sensitive, private, and confidential information may include, but is not limited to, student or staff Personally-Identifiable Information (PII), Protected-Health information (PHI), student records, and employee data.

D. Users are required to follow all Office of Cybersecurity (OCS) policies and procedures when engaging with new vendors, or vendors that have not been vetted previously by OCS.

E. Users shall not reveal their passwords to anyone and shall take reasonable measures to protect their account credentials. Users are prohibited from using passwords or accounts other than their own.

F. Users are prohibited from logging into FCPS-issued devices with administrator privileges.

G. Designated users must maintain multi-factor authentication (MFA) at all times to use FCPS Core systems.

H. Users are prohibited from accessing portions of the internet that are inconsistent with the educational or instructional mission or administrative function of FCPS.

I. Users shall not download copyrighted materials from the internet or further transmit such materials in any form without compliance with all terms of a pre-authorized agreement. FCPS will not tolerate infringement or violation of the United States or international copyright laws and/or restrictions.

J. Any use of FCPS technology resources for personal use unrelated to the mission of FCPS or private gain shall be kept to a minimum. Users are prohibited from using the FCPS network to market commercial products and services. Staff development activities are considered FCPS mission related.

K. Users are prohibited from using FCPS resources to commit, facilitate, encourage, and/or promote illegal acts.

L. Users are prohibited from knowingly sending, receiving, viewing, downloading, and/or publishing illegal material via the internet, including social media, such as but not limited to, 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 activities, or that is considered child pornography.

M. Users are prohibited from using FCPS technology resources to harass or threaten individuals or groups.

N. Users are prohibited from installing any software that is not approved by FCPS, as outlined in Regulation 3008 for instructional software and Regulation 6710 for administrative software. Any software or application deemed unsafe by the Office of Cybersecurity (OCS) shall not be approved.

O. Users are prohibited from vandalizing technology resources on the FCPS network or using FCPS resources to vandalize. This includes, but is not limited to, attempts to access, alter, and/or delete data of another user without proper authorization, endangerment of the integrity of information systems and/or resources, and any damage to equipment. The introduction of malware is an example of vandalism.

P. Users are prohibited from using FCPS technology resources to commit, facilitate, encourage, and/or promote the unauthorized or fraudulent use of a credit card.

Q. Users are prohibited from using FCPS technology resources to forge or interfere with electronic mail messages.

XI. INDIVIDUAL ACCEPTABLE USE POLICY REGULATION

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

B. Schools will review the AUP with students and enforce rules of conduct necessary to foster appropriate student use of technology resources. Schools shall require that all students and parents sign Attachment A, AUP Student Network Access, and retain a copy of the signed document in the school's main office.

C. Central offices will educate staff members on personal safety practices and effective techniques for identifying and evaluating information and its sources. FCPS employees and contractors shall read and comply with guidelines in Attachment B, AUP Staff Member and Contractor Computer Systems and Network Access.

D. Use of FCPS technology resources is contingent upon acceptance of the terms of an AUP and compliance with the rules set forth therein, as well as applicable School Board policies, regulations, and the Student Rights and Responsibilities.

XII. REPORTING REQUIREMENT

A. If any FCPS employee, student, or network user becomes aware of inappropriate use of technology 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.

B. Any user shall promptly report to a school principal or program manager:

1. Loss and/or theft of any FCPS-owned device.

2. Knowledge and/or suspicions of unauthorized access to FCPS-owned devices and/or electronic records.

3. Knowledge and/or suspicions of unauthorized disclosure of confidential electronic records.

4. Knowledge and/or suspicions of the use of FCPS technology resources to access materials that are obscene, harmful to juveniles, threatening or harassing, and/or material that constitutes child pornography.

5. Knowledge or suspicions of the use of FCPS technology resources to promote, encourage, and/or provide the skills to commit illegal activities.

6. Knowledge or suspicions of vandalism on the FCPS network or using FCPS resources.

7. Knowledge or suspicions of FCPS trademark infringement or entities fraudulently impersonating FCPS or disseminating misinformation about FCPS.

XIII. MONITORING AND DISCLOSURE OF INFORMATION

Users have no right or expectation of privacy for any activities conducted on FCPS technology resources, whether the device is on- or off-premises, including but not limited to browsing activity and email or materials sent, received, and/or stored on any division system.

School officials reserve the right to monitor and record all user activity. Any evidence of a violation of an AUP*,* School Board policy or regulation, and/or the Student Rights and Responsibilities will be provided to division administrators and may result in disciplinary action. Any evidence of the use of FCPS technology resources in violation of local, state, and/or federal laws, may result in disciplinary action and/or criminal prosecution.

Records stored or maintained in FCPS technology resources may be subject to disclosure under the Virginia Freedom of Information Act, in connection with any state or federal compliance action, in connection with litigation involving the School Board, or in response to a subpoena, search warrant, and/or court order.

XIV. **FCPS WEB PRESENCE**

A. The FCPS website is not a public forum or a limited public forum for any purpose.

B. Principals and program managers are responsible for the accuracy and appropriateness of materials posted on school or department web pages or other social media, and for ensuring that the material is consistent with the social media guidelines, web curator guidelines, and official information posted by the executive director, office of Communications and Community Relations.

XV. USE OF ELECTRONIC MAIL (EMAIL) BY AN EMPLOYEE ORGANIZATION

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

A. To obtain an FCPS email account, the organization shall:

1. Be certified under the School Board’s registration procedure.

2. Each year submit a written request to the assistant superintendent, DIT, for account creation or renewal.

B. The organization must comply with the requirements stated in Section X of this regulation.

C. Email communications transmitted by the employee organization via the FCPS email system may not directly contradict FCPS policies, regulations, or practices, shall clearly identify the employee organization as the sender and shall include the following disclaimer: These materials are neither sponsored nor endorsed by the Fairfax County School Board, the Division Superintendent, or any school.

D. Broadcast email messages are permitted by authorized individuals and groups.

E. Use of email to solicit nonmembers of the organization to become members is not permitted.

F. Use of email for mass mailings to nonmembers is prohibited.

G. Use of email to advocate the election or defeat of any candidate for any elective office internal or external to FCPS, to advocate the passage or defeat of any referendum question, or to advocate the passage or defeat of any matter pending before the Fairfax County School Board, the Fairfax County Board of Supervisors, the Virginia General Assembly, or the Congress of the United States is not permitted.

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

XVI. **DISCLAIMERS**

FCPS makes no warranties of any kind, express or implied, for the network services it provides. FCPS is not responsible for any damage users may incur, including loss of data due to delays, non-deliveries, mis-deliveries, equipment failures or service interruptions. FCPS is not responsible for the accuracy, nature, or quality of information gathered from the internet. FCPS is not responsible for personal property used to access division hardware or networks or the internet or for any personal financial obligations incurred while using internet access provided by the division.

FCPS is not responsible for any device or data loss, theft, damage or other associated costs of replacement or repair of a personal device as a result of a student participating in the Bring Your Own Device initiative or of any other person who uses a personally-owned device to access the FCPS network.

Legal References: Code of Virginia, Sections 2.2-3700-3715, 18.2-372, 18.2-374.1, and 18.2-390, 22.1-70.2

See also the current versions of: Regulation 2601, Student Rights and Responsibilities Booklet
Regulation 2610, Rules of Conduct and Disciplinary Procedures
Regulation 3005, Program and Supplemental Instructional Print Materials Identification, Evaluation, and Approval
Regulation 3009, Challenged Library and Instructional Materials Policy 6401, Use of FCPS Network and Internet Resources Regulation 3012, School Libraries
Regulation 6225, FCPS Information Security Policy
Regulation 7005, Management of Fairfax County Public Schools' Internet Presence Attachments

FAIRFAX COUNTY PUBLIC SCHOOLS

Acceptable Use Policy Regulation for Student Network Access

The information systems and internet access available through FCPS are provided in order to support learning, enhance instruction, and support school system business and educational practices.

FCPS information technology systems are operated for the benefit of all users in connection with the core mission of FCPS - the education of its students. The use of the FCPS network is necessary to provide all students with access, support, and opportunities to use provided tools and resources; and for students to interact with other students, teachers, and class content to support and enrich their learning experience. Users are prohibited from taking, or attempting to take, any action that might reasonably be expected to disrupt the operation of the network or equipment and/or interfere with the learning of students or the work of FCPS employees.

All-access to the FCPS network shall be preapproved by the principal or program manager. The school or office may restrict, suspend, or terminate any user's access, without prior notice, if such action is deemed necessary to comply with laws or regulations, protect the safety of others, or maintain computing availability and security. Disabling student access to FCPS instructional technology tools is a serious action that will be taken only when warranted.

Students are advised that the inappropriate use of FCPS technology resources is a violation of student disciplinary rules, regardless of where or when the inappropriate use occurs. As such, schools will respond to instances of inappropriate use by following normal disciplinary procedures, just as they would if the incident occurred in the physical classroom. Disciplinary action for inappropriate use of the FCPS network, systems, or devices may be imposed as stated in the FCPS Student Rights and Responsibilities (SR&R) document.

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

FCPS Instructional Environment

Students have the right to physical and virtual educational environments that are consistent with the characteristics outlined in the FCPS SR&R document. These rights include:

- The right to be treated with respect in online learning environments. Students who do not feel they are being treated with respect should talk to their teacher or the principal.

- The right to express beliefs and opinions respectfully in online environments without being interrupted or punished. Students may talk to their teacher or principal if they feel that a school decision is not fair.
- The right of a student to give his or her version of events when accused of violating this Acceptable Use Policy Regulation.
- The right to access, support, and opportunities to use the provided technology tools and resources that support learning.
- The right to use technology to interact with other students, teachers, and class content to support their learning in both the physical and virtual environments.

Students may exercise these rights and privileges as long as they do so in a manner that does not interfere with the rights of others or the schools' ability to provide a safe learning environment.

Respect for Others

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

- Using or not using devices as directed by the teacher.
- Being considerate when using school resources.
- Always logging off devices or apps after finishing work.
- Not deliberately attempting to disrupt system performance or interfere with the work of other users.
- Leaving equipment and rooms in good condition for the next user or class.
- Not accessing, changing, or deleting files belonging to others that are not explicitly shared with you.

Ethical Conduct for Users

It is the responsibility of the user to:

- Use only his or her account or password. It is a violation to share passwords or to otherwise give access to an account to any other user. User account access is limited to currently enrolled students. Account access is not available to former students.
- Recognize and honor the intellectual property of others; comply with legal restrictions regarding plagiarism and the use and citation of information resources.
- Cite and credit all material used, including internet material.
- Only use software or apps on FCPS devices or networks that have been approved and that the school may legally use. Duplicating or modifying copyrighted software in violation of a license agreement is a serious offense that may result in student discipline.
- Use the FCPS technology resources in a manner that is consistent with the educational mission of the school system.
- Help maintain the integrity of the school information systems. Tampering or experimentation is not allowed; this includes the use of the FCPS network and resources to illicitly access, tamper with, or experiment with systems inside and outside FCPS.
- Help maintain a safe, positive, and trusting learning environment by not using offensive, obscene, or harassing language when on the FCPS network and/or FCPS devices.

Digital Citizenship and Security

- Students are responsible for complying with all cybersecurity policies set-forth by the Office of Cybersecurity (OCS).
- Students are prohibited from tampering with FCPS technologies and attempting to circumvent security policies and controls enforced by the Office of Cybersecurity (OCS), such as, but not limited to, accessing the internet via proxy or unauthorized VPN services.
- Students are prohibited from posting information if it violates the privacy of others, jeopardizes the health and/or safety of students, is obscene or libelous, intended to be threatening, bullying or hateful in nature, or causes disruption of school activities.
- Students may not access social media sites during school hours except where allowed by school administration. If allowed, social media activity must be limited to academic activities.
- Students are prohibited from accessing any portion of the internet that is inconsistent with the educational mission of FCPS.
- Students are prohibited from using phones, tablets, and other mobile devices in restrooms and locker rooms, unless there is a medical necessity or emergency.
- Students may utilize real-time messaging and online chat only within approved instructional apps or with the permission of the teacher or principal.
- Students are not to record electronically instructional programs, the classroom environment generally, or any conversation involving a school official, without the official's advance permission to do so.
- Students may not take photographs or videos of others without consent during school hours while on school property, unless for academic use. School administration may allow limited non-academic use of photography on a case-by-case basis.
- Students, under five years of age, are required to have adult-supervision while using FCPS technologies.
- Parents and/or guardians should ensure that use of student assigned devices is limited to supporting the educational outcomes of the student at home and the device not be used by anyone else for non-educational purposes.
- Students are not to reveal personal information (last name, home address, phone number) in correspondence with unknown parties.
- Students shall accept the responsibility for all material they access.
- Students are responsible for reporting any inappropriate material they receive.
- All student-produced web pages are subject to approval and ongoing review by responsible teachers and/or principals. All publicly-accessible web pages shall reflect the mission and character of the school.
- Students are prohibited from viewing, sending, and accessing illegal material.
- Students are prohibited from downloading inappropriate or illegal material on FCPS computers or networks.
- Students may not modify or rearrange keyboards, monitors, printers, or any other peripheral equipment.
- Students should report equipment problems immediately to a teacher, technical support staff, or principal.

- Students should leave desktop workstations and peripherals in their designated places.
- To ensure student safety and compliance with this Acceptable Use Policy Regulation, FCPS reserves the right to monitor and investigate students' online activities as needed. This includes accessing, reviewing, copying, storing, or deleting any communications or files so they can be shared with adults as necessary and as permitted or required by law. Students should have no expectation of privacy regarding their use of FCPS equipment, network, internet access, files, or email access.

Personally-Owned Computing and/or Network Devices (BYOD)

Students using personally-owned electronic devices must follow the policy stated in this document while on school property, attending school-sponsored activities, or using the FCPS network.

- Students using a personally-owned device with a wireless connection are only permitted to connect to the FCPS Wi-Fi network (not private cellular services) while on FCPS premises.
- When applicable, appropriate virus-checking software must be installed, updated, and made active prior to any personally owned device being placed on the FCPS network.
- No device placed on the FCPS network can have software that monitors, analyzes, or may cause disruption to the FCPS network.
- FCPS is not responsible for any device or data loss, theft, damage, or other associated costs of replacement or repair of a personal device as a result of a student participating in the BYOD initiative.
- FCPS staff will not be responsible for storing, supporting, or troubleshooting personal devices.
- Students will take full responsibility for any personally-owned device and will appropriately secure all devices when not in use.
- FCPS reserves the right to monitor and investigate all devices and activities on the FCPS network. The device may also be confiscated by school officials in accordance with the SR&R.

See also the current versions of: Regulation 6410, Appropriate Use of Fairfax County Public Schools' Network and Internet Resources
Regulation 2601, Student's Rights and Responsibilities Book

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

> *The technology resources provided by FCPS are provided in order to support learning, enhance instruction, and support school system educational practices.*

Employees, contractors, and volunteers shall read and comply with FCPS policies and regulations regarding use of its technology resources.

FCPS information technology systems and resources are operated in support of the educational mission of the school system. Users are prohibited from taking, or attempting to take, any action that might reasonably be expected to disrupt the operation of the network or equipment, interfere with the learning of students, or impair the work of other FCPS employees.

The principal or program manager determines who may have access to the FCPS network, and he or she may restrict, suspend, or terminate any user's access, without prior notice, if such action is deemed necessary to maintain technology availability, ensure appropriate use, or protect security. The principal or program manager may discipline any individual who violates this policy or school system regulations.

Property Ownership

FCPS technology 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 technology 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 may result in disciplinary action. Having a copy of software does not constitute authorization for modifications or duplications. Installing unlicensed software is not permitted. Users shall:

- 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 keycaps, 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 technology 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.

Conducting FCPS Business

A. Transparency of Records

- FCPS has a legal obligation to ensure that all records of FCPS official business are accessible to the public as required by the Virginia Freedom of Information Act and the Library of Virginia record retention rules. Emails, texts, or other electronic records that involve the performance of your duties as an FCPS employee, regardless of whether they are stored on the FCPS network or a personal device or account, may be considered public records and may be subject to disclosure under the Freedom of Information Act, the Family Educational Rights and Privacy Act, in connection with a compliance investigation, litigation, or a court order. As public records, they are subject to the same retention and maintenance requirements as any other record held by FCPS.
- Only FCPS email accounts or other FCPS-issued communication devices may be used to perform FCPS work duties and that any electronic records created that reflect FCPS official business must be stored on the FCPS network or FCPS-owned devices.
- Employees are not permitted to use personal email accounts or use personal devices such as tablets and smartphones to text or otherwise send or receive messages to carry out their job duties. Any messages received or stored on personal devices must be promptly forwarded to, or otherwise stored in an official FCPS account, device or on the FCPS network. No FCPS work products or other FCPS records, electronic or hard copy, may be stored at employees' homes, in personal PCs or other devices, or other places outside the control of FCPS.
- Any employee who maintains such FCPS records outside of the FCPS technology resources, will be required to cooperate immediately with FCPS requests for access to such records.

B. Use of FCPS Communication Systems such as Email Accounts, Texts, Messaging, and Chat

- FCPS communication systems shall be used primarily for FCPS business; personal use shall be incidental and minimal. Communication systems may not be used for financial gain, to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-FCPS purposes.

- Messages shall be professional and relate to FCPS business. 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 messages.
- Employees are responsible for all material maintained on their systems and in their accounts. If inappropriate or unsolicited material is received, it shall be deleted immediately. If it is repeatedly received and cannot be stopped, contact an SBTS or a TSSpec for assistance.
- Use real-time messaging and online chat only with the permission of a principal or program manager and only for school system business.
- As required by Regulation 4444, all electronic communications between employees and students shall conform to generally recognized professional standards in content and tone and be transparent and accessible to parents and supervisors. Private one-on-one electronic communications with individual students that are unrelated to school activities or any conduct that violates the law is inappropriate and prohibited.
- Employees are prohibited from using computers or the FCPS network to forge or interfere with electronic mail messages.

C. Security and Confidentiality

- Employees are responsible for complying with all cybersecurity policies set forth by the Office of Cybersecurity (OCS).
- Employees must only use assigned accounts, are prohibited from sharing passwords for network login or other individual accounts and must take proper precautions to protect account credentials. User account access is limited to currently employed staff. Account access is not available to former employees.
- Users shall maintain Multi-Factor Authentication (MFA) when accessing FCPS Core systems. FCPS users will not share their multi-factor keys with any user that is not an approved delegated user.
- Ensure devices are password and lock screen protected.
- In accordance with their roles, staff members, contractors, and volunteers may be granted access to personal information about FCPS employees or students that is confidential; they shall not disclose or discuss such information within FCPS except with the subject of the information or with individuals who have a legitimate business or educational need to know. Staff members, contractors, and volunteers shall not disclose this information to individuals or organizations outside FCPS unless they are entitled to it by law, policy, or legal process.
- FCPS users shall follow FCPS Data Security Guidelines. Sensitive information may not be stored in a local or removable device unless the data is encrypted.
- Promptly report to a principal or program manager:
    - Loss or theft of an FCPS-owned device.
    - Knowledge or suspicions of:
        - Unauthorized access to FCPS-owned devices or records.
        - Unauthorized disclosure of confidential records.
        - Use of FCPS technology resources to access materials that are obscene, harmful to juveniles, or that constitute child pornography.

- Use of FCPS technology resources to promote, encourage, or provide the skills to commit illegal activities.

D. Prohibited Activities

- Employees are prohibited from tampering with FCPS technologies and attempting to circumvent security policies and controls enforced by the Office of Cybersecurity (OCS), such as but not limited to, accessing the internet via proxy or unauthorized VPN services.
- Do not use the FCPS technology resources to access any portion of the internet that is inconsistent with the educational mission of FCPS.
- 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 educational mission. Remember that anything sent or posted on a school system computer is identifiable as originating from FCPS and reflects on the school system.
- Recognize and honor the intellectual property of others. Do not plagiarize. Comply with legal restrictions regarding the use and citation of others' work. Copyrighted materials shall not be downloaded from the internet or further transmitted in any form without compliance with applicable laws and terms of a pre-authorized agreement.
- Do not use FCPS technology resources to solicit or proselytize for commercial ventures or religious or political causes.
- Do not use offensive, obscene, libelous, or harassing language when using any FCPS technology resources.
- All users are prohibited from using FCPS technology resources to commit, facilitate, encourage, or promote illegal acts.
- All users are prohibited from using FCPS technology resources to harass or threaten individuals or groups.
- All users are prohibited from using FCPS technology resources 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 activities; or that is child pornography.
- Users are prohibited from vandalizing technology resources on the FCPS network or using FCPS resources. Vandalism includes any attempt to compromise the confidentiality, integrity, or availability of any technology resources, including but not limited to, attempts to access, alter, or destroy data of another user without proper authorization, damage to equipment, attempts to access or alter system data or files without proper authorization. The introduction of malware is an example of vandalism.

E. Special Rules Applicable to Non-Exempt Employees under the Fair Labor Standards Act

- Non-exempt FCPS employees cannot work more than 40 hours per work week without receiving overtime pay. Consequently, nonexempt users may not use FCPS technology resources, including the Virtual Private Network (VPN) system, to conduct FCPS business outside their regular work hours unless they have a supervisor's advance permission to do so.

F. Monitoring

- Users have no right or expectation of privacy for any activities conducted on FCPS technology resources, including but not limited to email or materials sent, received and/or stored on any division system.
- FCPS has the right to monitor and record all user activities on the FCPS network or FCPS- issued devices, whether the device is on or off the FCPS network. FCPS reserves the right to deny access to FCPS technology resources to any person who does not comply with this Acceptable Use Policy (AUP) Regulation, School Board policy or regulation. Any evidence of a violation of this AUP, School Board policy or regulation by an employee may result in disciplinary action, up to and including termination. Any evidence of the use of FCPS technology resources in violation of local, state or federal law, may result in disciplinary action and/or criminal prosecution.

Disclaimers

- FCPS makes no warranties of any kind, express or implied, for the network services it provides. FCPS is not responsible for any damages users may incur, including loss of data due to delays, non-deliveries, mis-deliveries, equipment failures or service interruptions. FCPS is not responsible for the accuracy, nature or quality of information gathered from the internet. FCPS is not responsible for personal property used to access division hardware or networks or the internet, or for any financial obligations resulting from internet access provided by the division.