A. Purpose

Frederick County Public Schools (FCPS) makes a variety of technologies available to staff to assist them in the performance of tasks associated with their positions and assignments. The purpose of this regulation is to establish guidelines to help maximize the responsible use of technology, and minimize the likelihood of illegal, unethical, or inappropriate use of technology that could harm FCPS, its students, or its employees.

B. Background

FCPS leverages technology in nearly every facet of accomplishing its mission on behalf of the Board of Education (Board), parents, and the taxpayers of Frederick County. FCPS strives to appropriately leverage technology to create a safe & secure environment for staff and students every day. The use of technology continues to grow exponentially throughout the organization. With FCPS' ever-increasing reliance upon technology, it is essential that all staff understand that they share in the responsibility to conduct themselves appropriately in the digital environment and in the responsibility to safeguard FCPS, students, and staff, while using technology resources.

C. Definitions

1. "Confidential Information" is defined to mean non-public information that has been deemed to constitute Personally Identifiable Information (PII), Federal Tax Information (FTI), Protected Health Information (PHI), Payment Card Information (PCI), Privileged or Sensitive, as defined in paragraph C(3) below.

2. "Digital Technology in FCPS" or "Technology" is defined to mean, but is not limited to:
   a. Hardware such as, but not limited to servers, computers, laptops, tablets, and other hardware, infrastructure, and peripherals.
   b. Software such as, but not limited to operating systems, application software, mobile applications, and websites.
   c. Physical media such as, but not limited to flash drives, external drives, and printed materials.
   d. Data such as, but not limited to locally stored and online documents, emails, instant messages, voicemails, passwords, database records, and files.
   e. Accounts such as, but not limited to internally or externally accessed accounts, applications, tools, websites, databases, email, websites, social media, cloud services, and mobile applications.
   f. Communication such as, but not limited to internet, LAN, WAN, Wi-Fi, telecommunications, and cellular.
   g. New technologies as they become available.

3. "Personally Identifiable Information" (PII) is defined to mean information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. For example, PII may include the name of a student; an individual's Social Security number; driver's license or state ID numbers; passport numbers, financial account numbers, and biometric identifiers. In combination, PII may include: the name of a student's parent, guardian or other family member, a list of personal characteristics which would make it possible to identify the student with reasonable certainty, a student's assigned identification number, home email, home address, personal telephone number, citizenship or immigration status, medical information, last 4 digits of the Social Security number, date of birth and/or mother's maiden name. These examples are neither comprehensive nor complete, and each instance must be evaluated individually.

4. "Proactive Network Security Assessment" (PNSA) is defined to mean an audit designed to find security vulnerabilities that are at risk of being exploited and could cause harm to business operations or expose sensitive information.

5. "Public Information" is defined to mean information that has been declared publicly available by FCPS or Maryland state officials with the explicit authority to do so. This information can be freely disseminated to anyone without concern for potential impact to FCPS or the State of Maryland, its employees, or citizens.

6. "School Property" or "School Grounds" is defined to mean any school or other FCPS facility, including grounds owned or operated by FCPS, FCPS buses and other FCPS vehicles, chartered vehicles, and the facility and/or grounds of any FCPS-sponsored activity involving students.

7. "Staff", for the purposes of this regulation only, is defined to mean all persons working for or with FCPS who are formally or informally authorized to use FCPS technology. This includes full-time FCPS employees, part-time FCPS employees, and FCPS volunteers, interns, contractors, vendors, and user groups.

D. Procedures

1. **Technology Access and Use in Frederick County Public Schools.**
   a. Technology access will be provided for educational, instructional, work-related, and other purposes consistent with the educational mission of FCPS.
   b. FCPS adheres to the requirements of the Children's Internet Protection Act (CIPA) as well as all other applicable federal, state, and local laws, regulations, and policies. Measures are taken to block or filter internet access as required by CIPA.
   c. Data created or stored on technology covered under this regulation are the property of FCPS. The school system may monitor, audit, and review all accounts, data, and communications to ensure that staff are using technology in accordance with Board policies, FCPS regulations, and federal, state, and local laws, regulations, and policies. Staff should not expect that communications will be private.

d. Any sharing of PII for instructional purposes must be in accordance with guidelines provided by the System Accountability and School Administration Department (i.e., student data) or the Office of Human Resources (i.e., staff data), in collaboration with the Department of Technology Infrastructure (DTI), and in compliance with FCPS approved digital tool content platform.

2. **Staff Responsibilities.** To ensure the responsible use of technology in FCPS, all FCPS staff will:
   a. Use technology in an ethical, responsible, and legal manner for FCPS-related purposes only.
   b. Be responsible for their behavior when using technology and for all actions taken under their accounts.
   c. Immediately report inappropriate uses of technology to a supervisor.
   d. Show respect to themselves and others when using technology.
   e. Model safe and appropriate use of technology to their students.
   f. Assign Internet use to students as follows:
      i. Staff must pre-screen Internet sites that they assign to elementary students. Elementary students may not search freely on the Internet.
      ii. Secondary students may access the Internet as needed for educational purposes.
      iii. Staff supervision is required to the extent that adequate monitoring of student activities on the Internet is feasible.
      iv. Staff members assigning Internet use will ensure that such activities are applicable to the curricular needs and developmental level of the student(s).
   g. Keep data private:
      i. Keep personal information (such as phone numbers, mailing address, passwords) and that of others private.
      ii. Never divulge passwords, or otherwise allow access, to their accounts to anyone. Staff are required to disclose system, account, or file-level passwords upon formal request of a direct supervisor.
      iii. Only create, process, store, or transmit data with technology that has been approved by FCPS for that data type (e.g., do not store PII in Google Workspace, do not use Flash Drives for anything other than explicitly approved purposes, do not enroll student data into unapproved applications).
      iv. Be vigilant to not become victim to scams such as phishing or other forms of social engineering.
      v. Comply with FCPS Regulation 400-20, *Student Records*, the Family Educational Rights and Privacy Act (FERPA), and all other federal, state, and local laws, regulations, and policies regarding student data.
   h. Only use FCPS-approved technology. Follow the established approval processes to have new technology approved for installation.
   i. Be responsible for taking reasonable measure to prevent theft, loss, or damage to FCPS technology.
   j. Never access the accounts of others without administrative authorization.
   k. Never circumvent or disable filtering or other technology protection measures put in place by FCPS.

l. Never use technology while on school property that violates this regulation. Examples of violations may include, but are not limited to:
   i. Racism. (*See* Board Policy 117, *Anti-Racism*.)
   ii. Bullying/Harassment/Intimidation. (*See* Board Policy 309, *Discrimination and Harassment* and Board Policy 437, *Bullying/Harassment/Intimidation*.)
   iii. Sexual Harassment. (*See* Board Policy 116, *Title IX Sexual Harassment*.)
   iv. Denigration or defamation of character.
   v. Jeopardizing the safety of others.
   vi. Offensive, rude, threatening, or discriminatory behavior.
   vii. Accessing or distributing pornographic materials.
   viii. Spreading gossip and/or rumors.
   ix. Knowingly spreading viruses, worms, or any other malicious files.
   x. Violating copyright laws.
   xi. Installing or using unauthorized software
   xii. Accessing another individual's accounts, materials, information, or files without authorization.
   xiii. Unauthorized entry (*e.g.*, hacking).
   xiv. Advertising commercial products or services.
   xv. Sending mass unsolicited communications.
   xvi. Engaging in activities for personal gain or profit.
   xvii. Vandalizing, damaging, or disabling FCPS technology.

3. **Staff Instruction in Responsible Use of Technology** Every year staff will receive training in safe and responsible use of technology, including:
   a. FCPS Regulation 434-01, *Technology Use, Students*.
   b. FCPS Regulation 300-45, *Technology Use, Staff*.
   c. Digital Citizenship (Digital access, etiquette, law, communication, literacy, commerce, rights and responsibilities, safety and security, health and wellness).
   d. FCPS Regulation 500-29, *Copyright*.

4. **Proactive Network Security Measures.** To support employees with recognizing potentially malicious activity, FCPS will conduct Proactive Network Security Assessments (PNSA). These network security measures are an extension of the annual training staff receive each year and an important component in FCPS' legal compliance, data privacy, security, and insurance processes. An example of a PNSA could be a phishing email sent by members of DTI.

5. **Consequences of Violations**
   a. Staff who violate the terms of this regulation or fail PNSA will be provided with progressive discipline support to identify the behaviors and/or actions that resulted in the violation. Patterns of repetitive behaviors will follow the progressive disciplinary process. Supervisors should support their employees in gaining the necessary supportive measure to better understand responsible use of technology.
   b. Steps of the progressive discipline support process are outlined below:

i. First violation or failure of the PNSA will result in FCPS providing notification to the employee's direct supervisor. The supervisor is expected to make the employee aware of the actions and expectations.
ii. Second violations or failure of the PNSA will result in FCPS providing notification to the employee's direct supervisor and the requirement to retake the required appropriate training module(s). The supervisor will also provide the employee with a Memo to the Record in accordance with FCPS's progressive disciplinary practices.
iii. Third violations or failure of the PNSA will result in FCPS providing notification to the employee's direct supervisor. The supervisor, in consultation with the appropriate stakeholder departments, will conference with the employee and reassess if the employee's access to the FCPS network should be modified. The conference shall serve as a verbal warning in the employee's due process workflow. All subsequent violations of this regulation will adhere to the standard FCPS progressive disciplinary escalation practices.

c. The consequences associated with the violation will follow a progressive discipline support process. However, FCPS reserves the right to implement measures to address violations and security vulnerabilities as deemed necessary.
d. Violations of this regulation will reset after one (1) calendar year.
e. Employees are also encouraged to reference the FCPS Employee Code of Conduct relating to proper use of technology.
f. In addition, FCPS reserves the right to report any suspected illegal activities to the appropriate authorities.

6. **Liability**
   a. FCPS will not guarantee accuracy, quality, confidentiality, or availability of technology and will not be responsible for any technology that may be lost, damaged, or unavailable.
   b. Although FCPS filters Internet content to comply with CIPA, FCPS cannot completely control or censor illegal, defamatory, inaccurate, or potentially offensive materials, which may be available to users of technology.

E. Related Information

1. **Board Policy**
   a. Policy 115, *Responsible Use of Social Media*
   b. Policy 117, *Anti-Racism*
   c. Policy 116, *Title IX Sexual Harassment*
   d. Policy 305, *Conflict of Interests and Employee Ethics*
   e. Policy 309, *Discrimination and Harassment*
   f. Policy 437, *Bullying/Harassment/Intimidation*

2. **FCPS Regulations**
   a. Regulation 100-08, *Responsible Use of Social Media*
   b. Regulation 200-49, *Personally Identifiable Information (PII) for FCPS School Officials*
   c. Regulation 400-20, *Student Records*

d. Regulation 434-01, *Technology Use, Students*
e. Regulation 500-29, *Copyright*

3. **FCPS Resources**
   a. FCPS Employee Code of Conduct

4. **Federal Law**
   a. Children's Online Privacy Protection Act (COPPA), 15 USC § 6501, *et seq.*
   b. Electronic Communications Privacy Act
   c. Family Educational Rights and Privacy Act (FERPA), 20 USC § 1232(g)
   d. Title XVIII, Children's Internet Protection Act (CIPA), 47 USC §§ 254(h), (l)

5. **Maryland Law**
   a. Maryland Local Cybersecurity Act of 2022

6. **Maryland Statutes**
   a. Md. Code Ann., Crim. Law § 3-805
   b. Md. Code Ann., Labor & Emply. § 3-712

F. Regulation History (Maintained by Legal Services)

Responsible Office	Department of Technology Infrastructure
Adoption Dates	04/01/96
Review Dates	08/08/23, 01/03/24, 03/20/24
Revision Dates	08/30/17, 03/20/24, 06/04/24