FREDERICK COUNTY PUBLIC SCHOOLS	Reg. No. 300-45
Subject: RESPONSIBLE USE OF DIGITAL TECHNOLOGY - STAFF	Issued: 4/1/96
Preparing Office: Office of the Superintendent	Amended: 8/30/17

I. Policy

II. Procedures

A. Definitions

1. Digital Technology in Frederick County Public Schools (FCPS), hereafter referred to as "technology", includes but is not limited to:
   - Telephones, cell phones, and voicemail
   - Servers, computers, laptops, tablets, and other hardware, infrastructure, and peripherals
   - Software (operating system and application software)
   - Digitized information including locally stored and online files
   - Internally or externally accessed accounts, applications, tools, websites, or databases
   - FCPS-provided Internet access
   - FCPS-provided Wi-Fi
   - New technologies as they become available

2. "Staff" includes all adults 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.

3. Directory Information

   The student's name, participation in official recognized activities and sports, field of study, weight/height of members of athletic teams, honors/awards received, grade level, dates of attendance, teacher/class assignment, and/or the current school attended by the student, playbill or other program showing student roles in drama or music productions; and photographic, video or electronic images.

4. Personally Identifiable Information (PII) - COMAR 13A.08.02.03.B(13)

   "Personally identifiable" means that the data or information includes:

   a. The name of the student;
   b. The student's parent, guardian or other family member;
   c. The address of the student;
   d. A personal identifier, such as the student's Social Security number or student number;
   e. A list of personal characteristics which would make it possible to identify the student with reasonable certainty; or

f. Other information which would make it possible to identify the student with reasonable certainty.

NOTE: Any sharing of PII for instructional purposes must be in accordance with guidelines provided by the Department of Technology Infrastructure and in compliance with FCPS approved digital tool content platform.

B. Purpose

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.

C. Technology Access and Use in Frederick County Public Schools

1. Technology access will be provided for educational, instructional, work-related, and other purposes consistent with the educational mission of FCPS.
2. FCPS complies with the Children's Internet Protection Act (CIPA) and all other federal, state, and local laws and policies. Measures are taken to block or filter Internet access as required by CIPA.
3. Files and electronic communications created or stored on technology covered under this regulation are the property of FCPS. The school system may monitor, audit, and review all accounts, files, and communications to ensure that staff are using technology in accordance with FCPS regulations and federal, state, and local laws and policies. Staff should not expect that files or electronic communications will be private.

D. Staff Responsibilities

To ensure the responsible use of technology in FCPS, all FCPS staff will:

1. Use technology and their provided FCPS accounts in an ethical, responsible, and legal manner for school-related purposes only.
2. Be responsible for their behavior when using FCPS technology and for all actions taken under their digital accounts.
3. Show respect to themselves and others when using technology.
4. Model safe and appropriate use of technology to their students.
5. Assign Internet use to students as follows:
    a) Staff must pre-screen Internet sites that they assign to elementary students. Elementary students may not search freely on the Internet.
    b) Secondary students may access the Internet as needed for educational purposes.
    c) Adult supervision is required to the extent that adequate monitoring of student activities on the Internet occurs.
    d) Staff members assigning Internet use will ensure that such activities are applicable to the curricular needs and developmental level of the student(s).
6. Keep their personal data private:
    a. Keep personal information (such as phone numbers, mailing address, passwords) and that of others private.

b. Never divulge passwords, or otherwise allow access, to their digital accounts to anyone other than their FCPS supervisors. Staff are required to disclose system, account, or file-level passwords upon request of a supervisor.

7. Keep student data private:
    a. Comply with FCPS Regulation 400-20 *Student Records*, FERPA, and all other federal, state, and local regulations and policies regarding student data.
    b. Never post online, including social media, any information or images of students who have elected to opt out of "Directory Publish" on their Student Emergency Card.
    c. For safety reasons, student photographs posted online should never be labeled in a way that a viewer would know the student's full name or how to locate/contact them. Information and images captured during public events are exempt from this restriction.
    d. Only create student accounts or upload/enter Personally Identifiable Information into online applications that have been approved by FCPS central office and/or are under contract with FCPS to handle student data. Students should use the "Google sign in" option for these online applications when available.
    e. Only FCPS-approved software and apps may be installed on FCPS devices. Follow the FCPS established app/software approval process to have new apps and software approved for installation.
8. Never access the accounts of others without administrative authorization.
9. Never circumvent or disable filtering or other technology protection measures put in place by Technology Infrastructure.
10. Immediately report inappropriate use of technology to a supervisor.
11. Never create, access, use, or distribute digital content while using FCPS technology or while on FCPS property that violates this regulation. Examples may include, but are not limited to:
    - Bullying/Harassment/Intimidation (Board Policy 437)
    - Sexual Harassment (Board Policy 318)
    - Denigration or defamation of character
    - Jeopardizing the safety of others
    - Offensive, rude, threatening, or discriminatory electronic communications
    - Pornographic materials
    - Gossip and rumors that affect instruction
    - Knowingly spreading viruses, worms, or any other malicious files
    - Violating copyright laws
    - Installing or using unauthorized software
    - Accessing another individual's accounts, materials, information, or files
    - Unauthorized entry (hacking)
    - Advertising commercial products or services
    - Mass unsolicited communications
    - Using FCPS technology for personal gain or profit
    - Vandalizing, damaging, or disabling FCPS technology
12. Staff is responsible for taking reasonable measures to prevent theft, loss, or damage to FCPS technology.

E. Staff Instruction in Responsible Use of Technology

Every year staff will receive training in safe and responsible use of technology, including:

- FCPS Regulation 400-73: *Responsible Use of Digital Technology - Students*
- FCPS Regulation 300-45: *Responsible Use of Digital Technology - Staff*
- Digital Citizenship (Digital access, etiquette, law, communication, literacy, commerce, rights and responsibilities, safety and security, health and wellness)
- FCPS Regulation 500-29: *Copyright*

F. Consequences of Violations

Violations of this regulation will subject the violator to disciplinary action in accordance with FCPS disciplinary policies. In addition, FCPS reserves the right to report any suspected illegal activities to the appropriate authorities.

G. Liability

1. FCPS will not guarantee the availability of access to technology 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 online resources cannot be guaranteed.
3. 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 FCPS technologies.

Approved:

Original signed by

_____

Theresa R. Alban
Superintendent