A. Policy Purpose

1. To establish a data governance framework for technology security standards within Frederick County Public Schools (FCPS).

2. To establish countywide data privacy standards.

B. Definitions

1. "Adult Personally Identifiable Information" (APII) 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 lined or linkable to a specific individual. The definition of APII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available – in any medium and from any source – that, when combined with other available information, could be used to identify an individual.

2. "Confidential Information" is defined to mean non-public information that has been deemed to constitute Personally Identifiable Information (PII) (*i.e.*, APII and SPII), Federal Tax Information (FTI), Protected Health Information (PHI), Payment Card Information (PCI), Privileged or Sensitive information as defined below.

3. "Data Security" is defined to mean administrative, physical, and technical safeguards designed to protect FCPS's confidential information's confidentiality, integrity, and availability throughout its lifecycle, from creation or collection through destruction.

4. "Education Records" or "Student Records" is defined to mean records, files, documents, and other materials which contain information directly related to a student and are maintained by the Board through its institutions of elementary and secondary education, or by a person acting for the Board. Student records do not include the personal notes or records made by instructional, supervisory, and administrative personnel, and educational personnel ancillary thereto, which remain in the sole possession of the maker and which are not accessible or revealed to any other individual.

5. "Federal Tax Information" (FTI) is defined to mean tax information received directly from the Internal Revenue Service (IRS) or obtained through an authorized secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement, Bureau of the Fiscal Service, Centers for Medicare and Medicaid Services, or another entity acting on behalf of the IRS pursuant to IRC 6103(p)(2)(B).

6. “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.

7. “Payment Card Information” (PCI) is defined to mean personal data associated to an individual (cardholder) that uses credit, debit and/or cash cards for monetary transactions. PCI data includes account numbers, Social Security numbers, Date of Birth, and mailing addresses that associates a cardholder to a given payment account. Any information system that stores, processes, and/or transmits this data type must comply with the Payment Card Industry – Data Security Standard (PCI-DSS) control requirements to ensure cardholder data is appropriately protected from theft and fraudulent activities.

8. “Privileged Information” is defined to mean records that are protected from disclosure, and may include, but is not limited to, records:
    a. Relating to budgetary and fiscal analysis, policy papers, and recommendations made by FCPS or by any person working for FCPS;
    b. Provided by any other Maryland or Frederick County agency to FCPS in the course of FCPS’s exercise of its responsibility to prepare and monitor the execution of the annual budget;
    c. Relating to FCPS procurement, when a final contract award has not been made or when disclosure of the record would adversely affect future procurement activity; and
    d. Of confidential advisory and deliberative communications relating to the preparation of management analysis projects conducted by FCPS pursuant to the State Finance and Procurement Article of the Maryland Annotated Code.

9. “Protected Health Information” (PHI) is defined to mean health data created, received, stored, or transmitted by FCPS and their associated entities in relation to the provision of healthcare, healthcare operations and payment for healthcare services. PHI includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or health care coverage. PHI information is governed in accordance with the requirements prescribed by the Health Insurance Portability and Accountability Act (HIPAA). FCPS information systems that store, process, and/or transmit this data type must comply with the Health Insurance Portability and Accountability Act (HIPAA) control requirements (CFR Title 45 - Subtitle A -Subpart C - Part 164) to ensure reasonable administrative, technical, and physical safeguards are in place to prevent intentional or unintentional use or disclosure of PHI.

10. "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 and can freely be given to anyone without concern for the potential impact to FCPS or the State of Maryland, its employees or citizens.

11. "Record" is defined to mean any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

12. "Sensitive Information" is defined to mean information that, if divulged, could compromise or endanger the citizens or assets of Frederick County or the State of Maryland.

13. "Student Data" is defined to mean any personally identifiable information relating to an identified or identifiable student in the State.

14. "Student Personally Identifiable Information" (SPII) is defined to mean information that alone, or in combination, makes it possible to identify an individual student with reasonable certainty. The term includes, but is not limited to:
    a. The student's name;
    b. The name of the student's parent or other family members;
    c. The address of the student or student's family;
    d. A personal identifier, such as the student's social security number, student number, or biometric record;
    e. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
    f. Other information that alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
    g. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

C. Policy Statement

1. The Board of Education (Board) is committed to ensuring that the operation of FCPS information technology systems meets the necessary security controls and standards ensuring reasonable protection for the confidentiality, integrity, and availability of the data for which FCPS is responsible.

2. The Board is committed to ensuring that the operation of FCPS websites, online services, and applications designed for preK-12 school purposes are protected from unauthorized access, destruction, use, modification, or disclosure.

D. Implementation

1. The Superintendent is directed to develop guidance for all FCPS staff to implement and

maintain appropriate security procedures and practices to ensure student and staff confidential information and educational records are governed in alignment with best-practices and all applicable federal, State, and local laws, regulations, and legal and ethical requirements, as well as Board policy and FCPS regulation.

2. **Written Information Security Program (WISP)**
   a. The Superintendent is directed to develop and maintain appropriate guidance for FCPS staff to implement and maintain a Written Information Security Program (WISP) for FCPS information governance.
   b. The FCPS WISP will address the management, operational, and technical controls necessary to collect, store, process, and leverage organizational, student, and staff information (public information, confidential information, and educational records) within acceptable risk tolerances and in compliance with the Maryland Local Cybersecurity Support Act of 2022. The resulting program will create a comprehensive approach to organizational data security and information privacy.

E. Related Information

1. **Board Policy**
   a. Policy 115, *Responsible Use of Social Media*
   b. Policy 207, *Data Breach*
   c. Policy 305, *Conflict of Interests and Employee Ethics*
   d. Policy 421, *Student Education Records*
   e. Policy 500, *Approval of Curriculum and Instructional Materials*

2. **Code of Federal Regulations (CFR)**
   a. 34 CFR Part 98
   b. 34 CFR Part 99
   c. 45 CFR Part 164

3. **Code of Maryland Regulations (COMAR)**
   a. COMAR 13A.08.02, *Student Records*

4. **Decommissioned Board Policies**
   a. Policy 442, *Student Data Privacy*

5. **External Resources**
   a. Czuprynski, C. N., *Data Security for Schools: A Legal and Policy Guide for School Boards* (2019)
   b. Internal Revenue Service (IRS) Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies* (Rev. 11-2021)

6. **FCPS Regulations**
   a. Regulation 100-08, *Responsible Use of Social Media*
   b. Regulation 200-31, *Data Breach Response Process*
   c. Regulation 200-32, *Data Security*

d. Regulation 200-41, *Research Requests*
e. Regulation 200-42, *Maryland Public Information Act Requests*
f. Regulation 200-49, *Personally Identifiable Information (PII) for FCPS School Officials*
g. Regulation 300-02, *Telework*
h. Regulation 300-06, *HIPAA-Health Information-Electronic*
i. Regulation 301-03, *Technology Use, Staff*
j. Regulation 400-20, *Student Records*
k. Regulation 400-76, *Volunteer Involvement: Computer-Related Technology Guidelines*
l. Regulation 400-77, *Computers: FCPS Website Publishing*
m. Regulation 400-96, *Student Data Privacy*
n. Regulation 434-01, *Technology Use, Students*
o. Regulation 500-08, *Selection and Approval of Digital Tools for the Instructional Program*

7. **FCPS Resources**
   a. Device Permission Form

8. **Federal Law**
   a. Children's Internet Protection Act (CIPA)
   b. Children's Online Privacy Protection Act (COPPA)
   c. Electronic Communications Privacy Act
   d. Every Student Succeeds Act (ESSA), 20 USC § 7928
   e. Family Educational Rights and Privacy Act (FERPA), 20 USC §1232g
   f. Health Insurance Portability and Accountability Act (HIPAA), 42 USC § 1320d, *et seq.*
   g. Privacy Act of 1974
   h. Protection of Pupil Rights Amendment Act (PPRA), 20 USC §1232h
   i. Stored Communications Act

9. **Federal Statutes**
   a. 20 USC § 7928

10. **Maryland Law**
    a. Maryland Local Cybersecurity Support Act of 2022
    b. Maryland Online Data Privacy Act of 2024
    c. Maryland Public Information Act
    d. Maryland Student Data Privacy Act of 2015

11. **Maryland Statutes**
    a. Md. Code Ann., Coml. § 14-3501
    b. Md. Code Ann., Coml. § 14-3502
    c. Md. Code Ann., Coml. § 14-3503
    d. Md. Code Ann., Coml. § 14-3504
    e. Md. Code Ann., Coml. § 14-3505
    f. Md. Code Ann., Coml. § 14-3506
    g. Md. Code Ann., Coml. § 14-3507
    h. Md. Code Ann., Coml. § 14-3508

i. Md. Code Ann., Crim. Law § 3-805
j. Md. Code Ann., Educ. § 4-131
k. Md. Code Ann., Educ. § 7-2101
l. Md. Code Ann., Educ. § 7-2102
m. Md. Code Ann., Educ. § 7-2103
n. Md. Code Ann., Educ. § 7-2104
o. Md. Code Ann., Educ. § 24-707
p. Md. Code Ann., State Govt. § 10-1301
q. Md. Code Ann., State Govt. § 10-1302
r. Md. Code Ann., State Govt. § 10-1303
s. Md. Code Ann., State Govt. § 10-1304
t. Md. Code Ann., State Govt. § 10-1305
u. Md. Code Ann., State Govt. § 10-1306
v. Md. Code Ann., State Govt. § 10-1307
w. Md. Code Ann., State Govt. § 10-1308

F. Policy History (Maintained by Legal Services)

Responsible Office	Department of Technology Infrastructure
Adoption Dates	07/12/17
Review Dates	
Revision Dates	01/07/26