A. Purpose

To establish systemwide expectations regarding the collection, use, maintenance, disclosure, retention, and destruction of student data and personally identifiable information (PII) by Frederick County Public Schools (FCPS).

B. Background

1. FCPS is committed to the security and privacy of the various types of student data that may be obtained, stored, transmitted, or created through electronic means. To operationalize this commitment, and to meet requirements established under applicable federal and state laws and regulations, and Board of Education of Frederick County (Board) Policy 208, *Data Security*, FCPS will maintain reasonable security procedures and practices to protect student data and implement measures to protect student data from unauthorized access, destruction, use, modification, or disclosure.

2. FCPS collects, stores, and uses a variety of student data to personalize learning experiences, inform decision-making, adhere to legal reporting requirements, and support students in a multitude of ways. In doing so, FCPS recognizes its responsibility to be a diligent steward of that data and is committed to protecting all confidential information within its own information technology systems, as well as ensuring that operators of other systems through contract with FCPS meet and maintain reasonable security safeguards for the protection of student data, in compliance with all applicable federal and state law and regulations, Board policies, and FCPS regulations.

C. Definitions

1. "Covered information" is defined to include personally identifiable or sensitive data about a student, including but not limited to the student's education records; first and last name; home address and geolocation information; telephone number; email address or any other contact information; test results, grades, and evaluations; special education information; criminal, medical, and health records; Social Security number; biometric and socioeconomic information; food purchases; political or religious affiliations; text messages; student identifiers; search activity; photos; voice recordings; disciplinary information; online behavior or application-usage data when linked or linkable to a specific student; persistent unique identifiers; and any confidential information protected from release or disclosure under federal or state law or regulation.

2. "De-identification" is defined to mean the process of removing or obscuring any PII from student records in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them.

3. “Digital Tool Approval Process” is defined to mean the comprehensive process by which FCPS staff review and evaluate digital tools for curricular alignment, program requirements, data privacy, security, equity, and equivalent access requirements.

4. “Disclosure” is defined as permitting access to, or the release, transfer, or other communication of, PII contained in student records to any party, by any means, including oral, written, or electronic means.

5. “Eligible student” is defined as a student who has reached 18 years of age or is attending an institution of postsecondary education.

6. “Legitimate Educational Interest” is defined to mean when a school official needs to review a student’s education record in order to fulfill their professional responsibilities

7. “Parent” is defined to mean a biological or adoptive parent, a court-appointed custodian or guardian, a foster parent, or a caregiver (as defined by the Education Article of the Maryland Annotated Code or as designated by the United States Department of Health and Human Services, Office of Refugee Resettlement).

8. “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, and includes student education records protected under the Family Educational Rights and Privacy Act (FERPA).

9. “Record” is defined as any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

10. “School Official” is defined to mean any employee of the school system with direct responsibility for providing services to students and other school officials designated by the Superintendent through an inter-agency agreement.

11. “Sensitive Data” is defined to mean data that carries the risk of adverse effects from an unauthorized or inadvertent disclosure.

12. “Student Data” is defined to mean any personally identifiable information relating to an identified or identifiable student in the State.

13. “Student Records” are defined as records that are directly related to a student and maintained by FCPS or by a party acting for FCPS.

14. “Third-Party Service Provider” is defined to mean any entity, whether public or private, that provides services to the Board through a contract or agreement, excluding the Maryland State Department of Education (MSDE) or MSDE’s contractors and subcontractors.

D. Procedures

1. **Applicability**
   a. This Regulation applies to:
      i. All FCPS offices, schools, departments, and divisions that collect, maintain, access, transmit, disclose, or destroy Student Data.
      ii. All School Officials with access to Student Data.
      iii. All third-party service providers that receive Student Data through contract or agreement.
      iv. All FCPS responses to Maryland Public Information Act (MPIA) requests involving Student Data.
   b. This Regulation does not apply to publicly reported aggregate enrollment data that is required by federal or state law and that does not contain Student Data or PII, including enrollment counts disaggregated by gender or race/ethnicity.

2. **Use and Disclosure of Student PII**
   a. PII or other sensitive data may be collected, used, maintained, disclosed, and reviewed by the Board, an FCPS school, or office, or a school system official only when serving legitimate educational purposes related to educational decisions, legal compliance, reporting, or other lawful purposes.
   b. No PII or other sensitive data will be shared with third parties outside of legally compliant activities or as specifically authorized by law, unless that release of data is authorized by the student's parent or by an eligible student.
   a. Any sharing of PII for instructional purposes must be limited to FCPS personnel, authorized individuals, or approved third-party service providers who have a legitimate educational interest. Such sharing must follow DTI guidelines and comply with FCPS's Digital Tool Approval Process outlined in FCPS Regulation 500-08, *Selection and Approval of Digital Tools*.
   c. FCPS applies suppression rules to all publicly reported data and to responses to MPIA requests, unless an exception is required by law. Values less than 10 and percentages below 5% or above 95% are suppressed consistent with MSDE guidance. Publicly released reports include only aggregate, non-identifiable data.
   d. Publicly released reports shall not include PII and shall use Aggregate Data in such a manner that re-identification of individual students is not possible.
   e. De-identified data may be shared without the consent required by FERPA with any party for any purpose, including parents, general public, and researchers, typically in the form of aggregated data.

3. **Maintaining, Retaining, and Destroying Student PII**
   a. School officials will take reasonable steps to ensure that records/data involving PII are not left in plain view or otherwise unsecured, and active and archived files containing PII are not left in common areas.
   b. School officials shall not store PII on a device itself, such as a hard drive, mobile device of any kind, or external storage device, that is not located within a secure area.
   c. School officials shall not replicate documents and files containing PII and/or store them on unsecure devices.

d. School officials should lock or secure confidential information at all times.
e. **Transferring PII**
    i. PII may only be transferred to individuals or third-party service providers who possess a "need-to-know" or a legitimate educational interest and are approved by the Information System Owner.
    ii. School officials may share records/data involving PII with other FCPS school officials who have a legitimate need to know the information by DTI approved file share systems or other secure FCPS provided and approved software.
    iii. School officials must take reasonable steps to ensure that they do not mistakenly disclose any PII or other sensitive data to any unauthorized persons in or outside FCPS.
    iv. In the event a school official has to transport PII via laptop or other portable electronic device, the device shall be encrypted.
f. School officials must immediately report any inadvertent disclosures of PII to their direct supervisor or senior administrator as soon as possible.
g. **Destroying Student PII.** School officials shall destroy PII when no longer needed for an audit, evaluation, or enforcement of or compliance with federal or state legal requirements.

4. **Training and Data Privacy Requirements**
    a. All FCPS offices/departments that handle PII must complete annual training.
    b. External vendor and/or third-party service provider contracts will include requirements for PII data encryption**.**

5. **PII Violations and Enforcement**
    a. This Regulation is binding on all school officials, each of whom is responsible for ensuring the procedures and standards set forth in this Regulation are met when they engage in the collection, transfer, storage, and/or disposition of student PII.
    b. FCPS employees found to be in violation of this Regulation may be subject to disciplinary action, up to and including termination.

6. **Review.** FCPS will periodically review this Regulation to ensure it remains current and consistent with legal requirements and best practices.

E. Related Information

2. **Board Policy**
    a. Policy 208, *Data Security*
    (https://apps.fcps.org/legal/documents/208)
    b. Policy 404, *Student Rights and Responsibilities*
    (https://apps.fcps.org/legal/documents/404)
    c. Policy 421, *Student Education Records*
    (https://apps.fcps.org/legal/documents/421)
    d. Policy 438, *Test Administration and Data Reporting*
    (https://apps.fcps.org/legal/documents/438)

3. **Code of Maryland Regulations (COMAR)**
   a. COMAR 13A.08.01.02, *Student Records*
   (https://fcps-md.info/COMAR_13A-08-01-02)

4. **External Resources**
   a. Institute of Education Sciences, National Center for Education Statistics (NCES) (Dec. 2010), *Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting*
   (https://fcps-md.info/NCES_Aggregate_Reporting)
   b. Maryland State Department of Education (MSDE) (Rev. Jan. 2026), *Data Suppression Requirements for Public Reporting*
   (https://fcps-md.info/MSDE_Data_Suppression)
   c. U.S. Department of Education (DOE) (Rev. October 2012), *Frequently Asked Questions – Disclosure Avoidance*
   (https://fcps-md.info/US_DOE_Disclosure_Avoidance)
   d. U.S. DOE, Data Security: K-12 and Higher Education Webpage
   (https://fcps-md.info/US_DOE_K-12_Data_Security)

5. **FCPS Regulations**
   a. Regulation 209-02, *Retention, Access, and Disclosure of FCPS Video Recordings*
   (https://apps.fcps.org/legal/documents/209-02)
   b. Regulation 200-31, *Data Breach Response Process*
   (https://apps.fcps.org/legal/documents/200-31)
   c. Regulation 200-41, *Research Requests*
   (https://apps.fcps.org/legal/documents/200-41)
   d. Regulation 200-42, *Maryland Public Information Act Requests*
   (https://apps.fcps.org/legal/documents/200-42)
   e. Regulation 210-01, *Technology Acquisition*
   (https://apps.fcps.org/legal/documents/210-01)
   f. Regulation 301-03, *Technology Use, Staff* (formerly 300-45)
   (https://apps.fcps.org/legal/documents/301-03)
   g. Regulation 421-01, *Student Education Records* (formerly 400-20)
   (https://apps.fcps.org/legal/documents/421-01)
   h. Regulation 434-01, *Technology Use, Students*
   (https://apps.fcps.org/legal/documents/434-01)
   i. Regulation 438-01, *Test Administration and Data Reporting* (formerly 400-62)
   (https://apps.fcps.org/legal/documents/438-01)
   j. Regulation 500-08, *Selection and Approval of Digital Tools*
   (https://apps.fcps.org/legal/documents/500-08)

6. **FCPS Resources**
   a. FCPS / Academics / Digital Learning Experience
   (https://www.fcps.org/academics/digital_learning_experience)
   b. FCPS / Families & Students / Student Code of Conduct
   (https://www.fcps.org/families_students/student_code_of_conduct)

7. **Federal Law**
   a. Family Educational Rights and Privacy Act (FERPA) (https://fcps-md.info/FERPA_20_USC_1232g)
   b. Individuals with Disabilities Education Act (IDEA) (https://fcps-md.info/IDEA_20_USC_1400)
   c. Protection of Pupil Rights Amendment (PPRA) (https://fcps-md.info/PPRA_20_USC_1232h)

8. **Maryland Law**
   a. Maryland Law Cybersecurity Act of 2022
   b. Maryland Student Data Privacy Act of 2015

F. Regulation History (Maintained by Legal Services)

Responsible Office	Department of Information Technology; Assessment, Data Reporting, and Strategic Improvement
Adoption Dates	08/20/15
Review Dates	
Revision Dates	05/15/26; 11/09/26