FREDERICK COUNTY PUBLIC SCHOOLS	Reg. No. 200-49
Subject: PERSONALLY IDENTIFIABLE INFORMATION (PII) FOR FCPS SCHOOL OFFICIALS	**Issued:** 5/11/22
Preparing Office: Office of the Superintendent	**Amended:**

I. Policy 208

II. Purpose

To ensure comprehensive management of written and electronic records involving Personally Identifiable Information (PII) of Frederick County Public Schools (FCPS) school officials. This regulation addresses the lifecycle of PII collected, stored, accessed, transferred and disposed of by FCPS, and the steps necessary to minimize the likelihood of inappropriate disclosure of confidential PII.

III. Definitions

Information System Security Inventory of PII - documents all automated information systems associated within a security boundary that contains PII (Staff & Student) and FCPS Sensitive Information.

DTI staff – employees of the FCPS Department of Technology Infrastructure.

Personally Identifiable Information (PII) - 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. It requires a case-by-case assessment of the specific risk that an individual can be identified. For example, PII may include 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: 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.

School officials – all adults working for or with FCPS who are formally or informally authorized to receive, store, process or transmit FCPS-owned data, whether the system is hosted on the FCPS network or by a third-party provider. This may include employees, Board of Education members, volunteers, interns, contractors, vendors, and user groups.

Written Information Security Program (WISP) – The WISP is described in detail within the FCPS DTI Information System Security Manual (ISSM).

IV. Procedures

A. Collection of PII

1. School officials should collect, use, and retain only relevant PII necessary for the original purpose for which it was collected. The access, use, and sharing of FCPS data should be limited to the least possible quantity necessary to complete the legitimate educational or business requirement of FCPS. Data processing should only use as much data as is required to successfully accomplish a given task.
2. Information systems used to collect PII must be listed in the Information System Security Inventory of PII.
3. DTI staff shall take steps to provide in-transit and at-rest encryption security for all electronic data/records involving PII.
4. Electronic handling of records/data involving PII is strictly limited to those individuals specifically assigned such responsibilities.
5. 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. Storage of PII

1. Information System Owner shall take steps to ensure that computers housing PII data will be made physically inaccessible to unauthorized users.
2. 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.
3. DTI staff will take steps to routinely monitor computer systems and devices used to store or access PII for unauthorized use, possession or access.
4. School officials shall not replicate documents and files containing PII and/or store them on unsecure devices.
5. School officials should lock or secure confidential information at all times.
6. At the end of each workday, school officials shall secure all files and other records containing PII in a manner that is consistent with departmental requirements and/or these procedures.
7. Visitors will not be permitted to visit unescorted any area within FCPS premises that contain records/data involving PII.
8. Digital PII will only be stored on technology storage media secured with encryption compliant with the latest versions of NIST 800 series guidance.

C. Access to PII Data

1. DTI staff will take steps to limit access to electronically stored PII to those employees having a unique log-in ID.
2. School officials shall not access, keep, or use PII from or on a non-district designated device.
3. DTI staff will take steps to ensure that PII in a digital format is only viewed on secure FCPS authorized devices, unless being accessed by the source of the PII data.
4. Information System Owner will take steps to periodically review system access to ensure access privileges are removed once the data/records involving PII are no longer required for legitimate purposes.

5. School officials shall not obtain, access, keep, use, or view any PII without authorization from a supervisor. When in doubt, school officials should ask for authorization by senior administrators before accessing confidential PII.
6. Re-log-in is required when the computer is not in use, in a manner compliant with the Session Lock requirements of the FCPS DTI ISSM.
7. In accordance with FCPS Regulation 300-45 *Responsible Use of Digital Technology – Staff*, any school official who has access to PII shall not share their electronic passwords for computer and electronic records access.
8. All information systems storing PII should employ Multifactor Authentication (MFA), where technically feasible. If the use of MFA is determined by the Director of Technology Infrastructure to be inappropriate or one of the factors of authentication is decided to be a password, the password must meet the complexity requirements as outlined in DTI's Information System Security Manual.
9. School officials may only grant access to PII for individuals or vendors who possess a "need-to-know" or a "legitimate educational interest" and are approved by the Information System Owner.

D. Transferring PII

1. PII may only be transferred to individuals or vendors who possess a "need-to-know" or a "legitimate educational interest" and are approved by the Information System Owner.
2. School officials may share records/data involving PII with other FCPS school officials who have a legitimate need to know the information, by using the file share system (e.g. H/K/R/U/V drives) or other secure FCPS provided and approved software (e.g. PeopleSoft).
3. School officials must take reasonable steps to ensure that they do not mistakenly disclose any confidential information to any unauthorized persons in or outside FCPS.
4. In those rare instances when a school official has to transport PII via laptop or other portable electronic device, the device shall be encrypted.
5. School officials must immediately report any inadvertent disclosures of PII to their direct supervisor or senior administrator as soon as possible.
6. DTI staff shall take steps to ensure that PII that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the FCPS network.

E. Disposition of PII

1. Upon retirement, resignation, termination or at any time upon the request of their supervisor or a senior administrator, all school officials shall surrender all organizational records/data involving PII to FCPS.
2. School officials shall destroy PII when it is no longer needed in compliance with record retention requirements.
3. DTI staff shall take steps to ensure a school official's remote electronic access to PII is disabled upon the date of retirement, resignation or termination.

F. Training and Audit Procedures

1. FCPS shall take steps to ensure school officials are trained to report lost or stolen equipment immediately, and how to report any observed or known violation of this regulation to a supervisor.

2. Initial PII awareness training for all new employees must be completed prior to the employee being granted access to data/records involving PII.
3. All FCPS offices/departments that handle PII must complete annual training.
4. External vendor and/or service provider contracts will include requirements for PII data encryption.

G. PII Violations

1. 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 data/records that include PII.

2. A violation of this regulation, such as one or more of the following, is considered serious:
    a. Unauthorized disclosure of PII;
    b. Unauthorized disclosure of a log-in code (User ID and password);
    c. An attempt to obtain a log-in code or password that belongs to another person;
    d. An attempt to use another person's log-in code or password;
    e. Installation or use of unlicensed software on FCPS technological systems that could breach PII;
    f. An attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.

3. Depending on the seriousness of the infraction, an employee may face disciplinary action up to and including termination of the employment relationship. Failure by volunteers, vendors and outside affiliates to comply with these procedures may result in termination of the affiliation.

4. In cases where local, state, or federal laws have been violated, violators of these procedures may also face prosecution.

Cross-reference:

FCPS Regulation 200-32 *Data Security*
FCPS Regulation 200-41 *Research Requests*
FCPS Regulation 300-45 *Responsible Use of Digital Technology - Staff*

Approved

Original signed by

_____
Michael Markoe
Interim Superintendent