ADMINISTRATIVE PROCEDURE

CONFIDENTIAL DATA AND PERSONALLY IDENTIFIABLE INFORMATION (PII)

3050

Procedure No.

December 13, 2019

Date

1. **PURPOSE**: This procedure outlines requirements for employees of Prince George's County Public Schools who may have access as part of their job duties to confidential data, including personally identifiable information regarding current or former students, parents, staff, donors, and volunteers.

II. **BACKGROUND:**

In accordance with federal law, state law and Board Policy, PGCPS will make every effort to keep student records, personnel records and other types of confidential data safeguarded from unauthorized use or disclosure to individuals without a legitimate need to access the information.

III. **DEFINITIONS:**

A. Confidential Information:

Information maintained by PGCPS that (1) includes personally identifiable information regarding students, parents, staff, contractors or volunteers; or (2) would not be available to an individual under the Maryland Public Information Act.

Confidential information includes, but is not limited to: personal financial information; records relating to legal matters; medical or psychological information; and, subject to limitations, certain commercial or financial transaction information, pending investigatory records or records relating to internal, executive-level recommendations.

B. Personally Identifiable Information:

Includes information within an education record for students or personnel record for employees (including contract employees) which would reasonably be considered an invasion of privacy if disclosed.

Examples of "personally identifiable information" include, but are not limited to: social security numbers; EIN; date of birth; race, nationality, ethnicity, origin, color, religious or political beliefs or associations; sex, sexual orientation, gender identity, marital status,

personal financial information, including credit card and debit card numbers, or financial or bank account numbers and routing information; driver's license numbers and state identification card numbers; medical records or health care history (including pharmaceutical records); employment history or criminal background records; and employee home contact information.

Such data combined with an individual's first and last name (or first initial and last name), or any other method of linking the information to the individual, qualifies as "personally identifiable information."

This definition does not apply to information designated as directory information by law or school system procedures.

IV. PROCEDURES

A. Employment and Access Control

1. Security and control of Confidential Information shall be the responsibility of each division.

2. During the course of employment, staff may have access to Confidential Information. Staff who are authorized to use or disclose Confidential Information also have the responsibility to safeguard access to such information by limiting access to those that are allowed by permission and/or by law.

3. Any Confidential Information, whether oral, written, or electronic, should be maintained with respect and in a manner that ensures its confidentiality. The unauthorized release of any such Confidential Information is a violation of this procedure and may result in possible legal liability for the employee or PGCPS.

4. All employees and contractors must safeguard access to the PGCPS network (including students, parents and staff) and refrain from disclosing usernames or passwords which would allow unauthorized access to PGCPS computer systems.

   Employees must immediately report to the Supervisor/Division

Chief (Help Desk) and Department of Information and Technology any suspected or actual use of their login by someone other than themselves.

B. Security Control of Documents and Confidential Information

To protect PII against inappropriate access, use, disclosure, or transmission, requires appropriate administrative, technical and physical safeguards.

These include, but are not limited to:

1. Physical safeguards: Storing documents containing PII in secured cabinets or rooms and ensuring that documents containing PII are not left on desks or in other locations that may be visible to individuals not authorized to access the PII.

2. Minimization: Storing only PII that is necessary for the functions of the specific office/department; reducing the amount of PII included in records (including redaction of financial account information, use of less sensitive substitutes such as partial SSN and the PGCPS Identifier); and minimizing aggregations of PII. The risk of unauthorized disclosure of access to PII increases with the amount of data.

   This also includes reducing the number and scope of repositories of PII (both physical and electronic copies) and only for the time period where a valid business need for the information exists.

3. Storage – Storing PII only as necessary for the PGCPS mission as permitted under the PGCPS policy. Division Chiefs are responsible for providing guidelines around where information can be scanned/stored (e.g. in hardcopy, on shared drives, on other media/devices) and how long information may be retained before requiring deletion or destruction).

   In addition, Division Chiefs are responsible for maintaining up-to-date inventory of stored or maintained documents, files, databases and data sets containing PII, and their contents. The Division of Information Technology may provide additional guidance requiring the availability of encryption for PII stored

on mobile devices, media or other at-risk devices such as public workstations.

4. Disposal: Rendering PII unreadable prior to disposal. For example, this may include shredding documents to include papers, erasing or wiping electronic files.

C. Authorized Disclosure of Confidential Information within PGCPS

1. Only individuals within PGCPS who are permitted under law and PGCPS procedure and have a legitimate "need to know" are authorized to access, use, transmit, handle or receive PII specifically related to the performance of his or her PGCPS job duties.

2. Employees are prohibited from accessing, using and/or disclosing personally identifiable information for any reason other than the legitimate performance of the individual's job duties or in ways that jeopardize the security of such information.

3. Employees may only share personal identifiable information: (a) with other employees who have a legitimate need to know in order to perform their job duties; or (b) with others, if prior written consent specifying the purpose and timeline for the disclosure is provided by the individual who is the subject of the record. Employees must consult with their supervisor (or designee) to discuss any questions or concerns regarding sharing personal identifiable information with other employees prior to disclosing the information.

4. Employees must immediately report to their supervisor and the Division of Information Technology any unauthorized use or disclosure of confidential personally identifiable information.

5. An employee's failure to adhere to the requirements of this procedure regarding protection of PII may result in disciplinary action up to and including termination of employment, and possible legal liability.

6. An employee's obligation to protect personally identifiable information continues after termination of employment. Any

misuse or unauthorized release of such information subsequent to the conclusion of employment with PGCPS may be grounds for legal action.

D. Permitted Disclosure to Third Parties

1. PGCPS may release PII to third parties only as permitted by law and PGCPS policy. Third party contractors to whom PGCPS is disclosing PII must be bound by agreements with appropriate PII safeguarding and use provisions.

2. "Directory information" regarding students or personnel may be released without prior permission in accordance with the law and PGCPS procedures.

   a. For students, Administrative Procedure 5134 defines "directory information" as the student's name; address; telephone listing; grade level; enrollment status; dates of attendance; participation in officially recognized activities and sports; honors and awards received; and the most recent school attended.

      However, this information should not be released without confirming with the school whether the parent/guardian submitted an "opt-out" notice of sharing the directory information without consent.

   b. For employees, directory information is generally considered the employee's name, title, work location, work contact information, public salary and public licensure information. Requests for any other information should be reviewed by the Office of General Counsel prior to release.

   c. Employees must consult with their supervisor (or designee) to discuss any questions or concerns regarding sharing directory information regarding students or employees prior to disclosing the information.

V. **TRAINING:**

Each manager, supervisor or principal of a PGCPS office, or department or school is responsible for an annual review of this procedure with staff regarding protection of PII. Sign-in sheets must be used to track the date, time and attendees for the annual review.

VI. **MONITORING AND COMPLIANCE**:

The Division Chiefs will be responsible for the monitoring and compliance for this procedure on an annual basis. The records shall be kept for at least three (3) years.

VII. **RELATED PROCEDURES**:

Administrative Procedure 0700 - Information Technology Services-Acceptable Usage Guidelines;
Administrative Procedure 0701 - Information Technology Services-Google Application Procedures
Administrative Procedure 5125 - Individual Student School-Based Records;
Administrative Procedure 5134 - FERPA Directory Information; and
PGCPS Employee Code of Conduct

VIII. **MAINTENANCE AND UPDATE OF THESE PROCEDURES**:

This procedure originates with the Chief Operating Officer and will be updated as needed.

IX. **CANCELLATIONS AND SUPERSEDURES**: None. This is a new procedure.

X. **EFFECTIVE DATE**: December 13, 2019