Administrative Procedures for Data Privacy
(Attachment for Policy No. 831)

Purpose

As a custodian of sensitive data belonging to students, employees, parents and other individuals, the Board of Education ("Board") recognizes its responsibility to safeguard this data from unauthorized use, disclosure, disruption, modification, or destruction. While data privacy can be compromised by human error, hardware malfunction, natural disaster, security breach, etc., and may not be completely preventable, the purpose of Policy 831 and its Administrative Procedures is to promote confidentiality, integrity, and availability of the information assets owned and operated by the School District of Philadelphia ("District"). These Administrative Procedures and the protocols linked within establish a framework for managing privacy risks in line with the NIST Privacy Framework and the Fair Information Practice Principles (FIPPs).

Definitions

Access: Viewing, editing, printing, downloading, copying or retrieving data from a computer, computer system, computer network or other medium.

Availability: The expectation that authorized users have access to information and IT services when required.

Confidential Data: Personally identifiable information about a student, parent/guardian, or employee that is prohibited from disclosure pursuant to state or federal law or information that is intended for the use of a particular persona/group and whose unauthorized disclosure could be harmful to the individual it identifies.

Confidentiality: The expectation that the information resource is only accessible to those with authorized access and that the information resource is protected throughout its lifecycle .

Fair Information Practice Principles (FIPPs): The Federal Privacy Council's widely accepted principles for evaluating information systems, processes, programs, and activities that affect individual privacy.

Information Asset: Any data, information, or IT service which hosts District data and/or information, in any format, that the District owns or manages and for which the District is responsible. This can include software, hardware, data, intellectual property, and personal information.

Integrity: The safeguarding of the accuracy and completeness of information contained in a record and the processing methods that are applied to a given piece of information or data set.

Lifecycle: The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.

National Institute of Standards and Technology (NIST): Agency of the United States Department of Commerce whose mission promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology.

NIST Privacy Framework: A voluntary tool designed to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy.

Personal Information: Any data that can identify an individual either directly or indirectly.

Privacy Risk: The potential for harm or adverse effects on individuals resulting from the collection, use, sharing or disposal of their personal information.

Sensitive Data: Information that, if disclosed, could result in harm to an individual.

Procedures

The Superintendent designates the Office of Information Security as responsible for implementing and maintaining the requirements of this policy and its procedures.

The District is committed to managing privacy risk to personal information across several domains: Identify; Govern, Control, Communicate and Protect as outlined in the National Institute of Standards and Technology (NIST) Privacy Framework. Under each domain, the Office of Information Technology and Data Management (OITDM) maintains protocols that take into account industry best practices and the Fair Information Practice Principles (FIPPs).

Where possible, these protocols are available to the public and linked below. However, several protocols remain confidential and accessible only to designated OITDM staff, in accordance with industry best practices. Publicly accessible protocols include details about providing training to users of District information assets and systems, where applicable.

Privacy Protection Domains:

Under each of the below privacy protection domains, the District has established specific operational protocols. These protocols, identified and briefly described below, outline how the District manages its privacy programs.

I. Identify

A. Data Inventory: Establishes a comprehensive inventory of personal information collected, processed and stored by the District.
B. Privacy Risk Assessment (Internal & Confidential): Defines the process for identifying, evaluating, treating and reporting privacy risks associated with the use of personal information.
C. Data Mapping (Internal & Confidential): Maps data flows to understand where personal information is collected, stored, processed and shared.

II. Govern

A. Privacy Policies and Procedures: Establishes comprehensive privacy policies and procedures aligned with the NIST Privacy Framework and FIPPs.
B. Roles and Responsibilities: Clearly defines roles and responsibilities regarding personal information protection. ***Internal and Confidential***
C. Training and Awareness: Provides all individuals within the District who have access to personal information with the necessary awareness, knowledge and skills to protect this information.
D. Vendor Management: Ensures all contracts with third-party vendors and service providers include data privacy and security language compliant with the District's privacy policies and standards.

III. Control

A. Access Control: Defines requirements for and controls user access to personal information. ***Internal and Confidential***
B. Change Management (Internal & Confidential): Establishes a coordinated method for managing changes to personal information handling practices to minimize potential negative impact on privacy.
C. Data Protection Measures: Outlines the responsibilities and procedures for the protection of personal information, including access controls, data minimization, de-identification, encryption and secure disposal. ***Internal and Confidential***
D. Privacy Impact Assessment (Internal & Confidential): Evaluates the privacy impacts of new or changed data processing activities.
E. Record Retention: Establishes protocols for the retention and secure disposal of personal information.

IV. Communicate

A. Privacy Notices: Develops clear and transparent communication channels to inform individuals about how their personal data is processed and protected.
B. Access Management: Establishes procedures that allow individuals to access, correct or request the deletion of their personal information.
C. Complaint Handling: Establishes procedures for receiving and addressing privacy-related complaints and inquiries from individuals.

V. Protect

A. Incident Response Plan (Internal & Confidential): Implements a comprehensive incident response plan to address data breaches, including notification to affected individuals and authorities as required.
B. Backup Procedures (Internal & Confidential): Establishes protocols for regular backup of personal data to ensure data recovery in case of loss.
C. Monitoring and Reporting (Internal & Confidential): Conducts regular monitoring and reporting of privacy controls to ensure ongoing compliance and identify potential vulnerabilities.
D. Encryption and Data Protection (Internal & Confidential): To provide guidelines for the proper handling, storage, and transmission of sensitive data using encryption and other data protection methods to help prevent unauthorized access or disclosure.
E. Privacy Audits (Internal & Confidential): Conducts regular privacy audits to assess compliance with privacy policies and procedures.

Maintenance Schedule

These Administrative Procedures and the protocols designated within shall be reviewed upon the review of the Policy, or upon the occurrence of a triggering event.

Related Information:

NIST Privacy Framework
NIST Cybersecurity Framework Tools
Fair Information Practice Principles (FIPPs)