NORTHERN WESTMORELAND CAREER AND TECHNOLOGY CENTER

No. 830.1

SECTION: OPERATIONS

TITLE: DATA GOVERNANCE – STORAGE/SECURITY

ADOPTED: March 20, 2025

REVISED:

Purpose

The center is required to collect, create, store and manage data and information. Accurately maintaining and protecting such data is essential for efficient center operations, legal compliance, confidentiality and upholding trust with the community.

This policy addresses the Joint Operating Committee's commitment to sound data governance related to the integrity and security of the data collected, maintained, stored and managed by the center.

Authority

The Joint Operating Committee recognizes the importance of establishing and maintaining a system of data governance that addresses staff responsibilities and complies with federal and state laws and regulations regarding data storage, security and records management. The center's data governance system shall meet or exceed industry and/or government standards for data protection and privacy of personal information.

The Joint Operating Committee directs that the creation, collection, retention, retrieval and disposition of the center's records shall be governed by Joint Operating Committee policy and the center's Records Management Plan and Records Retention Schedule.

The Joint Operating Committee directs notifications of a breach of the security of the center's computerized data system involving an individual's personal information to be conducted in accordance with law and Joint Operating Committee policy.

Definitions

Confidential Data/Information - information regarding which law, Joint Operating Committee policy or contract prohibit disclosure or that may be disclosed only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information and other personal information regarding students, employees and other individuals associated with the center.

Critical Data/Information - information that is essential to the center's operations and that must be accurately and securely maintained to avoid disruption to center operations.

Data Governance - the center's comprehensive system to ensure the integrity of data created,

collected, stored, secured and managed by the center.

Encryption - the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Personal Information - includes an individual's first name or first initial and last name in combination with and linked to any one or more of the following when not encrypted or redacted:

1. Social Security number.

2. Driver's license number or state identification card number issued instead of a driver's license.

3. Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

4. Medical information, meaning any individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional.

5. Health insurance information, meaning an individual's health insurance policy number or subscriber identification number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits.

6. A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

Records Management Plan - the system implemented by the center for the storage, retention, retrieval and disposition of all records generated by center operations.

Records Retention Schedule - a comprehensive listing stating retention periods and proper disposition of records.

Delegation of Responsibility

The Administrative Director, in collaboration with Business Manager shall develop procedures necessary to implement this policy.

All individuals who are granted access to confidential and/or critical data/information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of such data/information.

The Administrative Director shall conduct regular vulnerability and risk assessments to monitor the integrity of the center's system of data governance.

The Administrative Director shall ensure that this policy is reviewed at least annually and updated as necessary.

Guidelines

The center's system of data governance shall include, but not be limited to, the following:

1. Data security controls that meet or exceed industry and/or government standards for data protection and privacy, to ensure that only authorized individuals have access to computerized data.
2. A plan for backup and recovery of data to protect against information loss. Redundant backup systems of data storage shall be securely maintained in separate physical locations or in separate data storage systems.
3. Training requirements for individuals who have access to confidential and/or critical data and information.
4. Provisions to minimize the risk of unauthorized access, alteration or erasure of computerized data.
5. An inventory of all software applications, digital tools and platforms, and related instruments comprising the data governance system.
6. Procedures for addressing a breach of data and cybersecurity incidents.
7. Procedures and acceptable use provisions for access to data and protection of privacy and personal information for students, staff and other individuals associated with the center.
8. A requirement that all service providers retained or contracted by the center for data governance and records management purposes meet or exceed industry and/or government standards for data protection and privacy of personal information.

Use of Personal Electronic Devices and Resources

The center prohibits storage of confidential and/or critical data/information of the center on a personal electronic device, personal email account or other personal platform. Center staff and service providers shall use center-controlled accounts and platforms to securely access, store or transmit confidential and/or critical data/information of the center.

Service Providers

Service providers retained or contracted by the center shall comply with law, Joint Operating Committee policy, administrative regulations and center procedures regarding data security and integrity of data containing confidential and/or critical data/information of the center (school).

The center shall ensure that the agreement or contract for service with a service provider who may have access to confidential and/or critical data/information reflects appropriate data security provisions.

Consequences

Failure to comply with law, Joint Operating Committee policy, administrative regulations or procedures regarding data governance and security may result in the following disciplinary measures and possible pursuit of civil and criminal sanctions:

1. Employees may be disciplined up to and including termination.

2. Volunteers may be excluded from providing services to the center.

3. The termination of a business relationship with a service provider.

PSBA New 5/23 © 2023 PSBA

Legal References
1. 73 P.S. 2305.1
2. 73 P.S. 2305.2
3. Pol. 800
4. 73 P.S. 2301 et seq
5. Pol. 830
6. Pol. 113.3
7. Pol. 216
8. Pol. 324
9. 73 P.S. 2302
10. Pol. 801
11. Pol. 828
12. Pol. 815
13. Pol. 317
14. Pol. 818
15. Pol. 916