Policy

____ **Monitored**
____ **Mandated**
__X__ **Other Reasons**

DATA PRIVACY AND SECURITY

Purpose

The purpose of this policy is to outline essential roles and responsibilities within the West Orange Public Schools for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests. It also serves to establish a comprehensive data security program in compliance with applicable laws. This policy is also designed to establish processes for ensuring the security and confidentiality of information and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information.

Scope

This policy applies to all West Orange Public Schools offices, departments, and affiliated organizations including all employees, students, consultants, and vendors. For the purposes of this policy, affiliated organization refers to any organization associated with the West Orange Public Schools that uses district information technology resources to create, access, store, or manage district data including, but not limited to, assessment providers, food service providers, tutoring service providers, after school programs, etc. It also applies to any third party vendor creating, storing, or maintaining district data per a contractual agreement.

All district data must be classified according to the Data Classification Schema outlined below and protected according to applicable Data Security Standards. This policy applies to data in all formats and media.

Data Classification Schema

Data and information assets are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection. Three levels of data classification will be used to classify district data based on how the data are used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

Data are typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements. Consequently, the classification of the most sensitive element in a data collection will determine the data classification of the entire collection.

Data Visibility Classifications

Public - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the District, affiliates, or individuals. Public data generally have a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include:

1. District's public website
2. Directory information for students, faculty, and staff except for those who have requested non-disclosure (e.g., per the Family Educational Rights and Privacy Act (FERPA) for students)
3. Course descriptions
4. Semester course schedules
5. Press releases

Internal - Data intended for internal District business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data are generally not made available to parties outside the District. Unauthorized disclosure could adversely impact the District, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. Examples include:

6. Financial accounting data that does not contain confidential information
7. Departmental Intranet data
8. Information technology transaction logs
9. Employee ID numbers
10. Student ID numbers
11. Student educational records
12. Directory information for students, faculty, and staff who have requested non-disclosure (e.g., per FERPA for students.)

Confidential - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Steward is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the District, the personal privacy of individuals, or on compliance with federal or state laws and regulations. Confidential data have a very high level of sensitivity. Examples include:

13. Social Security Number
14. Personal identity information (PII)
15. Personnel records
16. Medical records

Roles and Responsibilities

Everyone with any level of access to district data is responsible for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function.

Every database system must have a Data Steward who is responsible for the quality, integrity, implementation, and enforcement of data management within their Organizational Unit. Data Managers are responsible for ensuring effective local protocols are in place to guide the appropriate use of data.

The following roles have specific responsibilities for protecting and managing district data and Data Collections:

Chief Data Steward(s) - Senior administration of the District responsible for overseeing all information resources: [1] Business Administrator (Custodian of Records), [2] Director of Technology (district data Coordinator)

Data Steward - Individuals responsible for overseeing a collection (set) of district data. They are in effect the owners of the data and therefore ultimately responsible for its proper handling and protection. Data Stewards are responsible for ensuring the proper classification of data and data collections under their control, granting data access permissions, appointing Data Managers for each district data collection, making sure people in data-related roles are properly trained, and ensuring compliance with all relevant policies and security requirements for all data for which they have responsibility. The Data Steward, having determined the category of the institutional data as confidential, will approve access based on appropriateness of the User's role and the intended use. Where necessary, approval from the Chief Data Steward(s) may be required prior to authorization of access.

Data Manager - Individuals authorized by a Data Steward to provide operational management of a district data collection. The Data Manager will maintain documentation pertaining to the data collection (including the list of those authorized to access the data and access audit trails where required), manage data access controls, and ensure security requirements are implemented and followed.

Data Processor - Individuals authorized by the Data Steward or designee and enabled by the Data Manager to enter, modify, or delete district data. Data Processors are accountable for the completeness, accuracy, and timeliness of data assigned to them.

Data Viewer - Anyone in the District or community with the capacity to access district data but is not authorized to enter, modify, or delete it.

Internal Audit Team - Performs audits for compliance with data classification and security policy and standards.

Student Data

The West Orange Public Schools classifies all student Personal Identifiable Information (PII) as private and confidential information. This type of data may be obtained, stored, and reviewed for legitimate educational purposes related to student achievement, accounting, pupil services, operations, compliance, and audit purposes. The maintenance and security of all student health records shall be in accordance with N.J.A.C. 6A:32-7.4 and 6A:16-2.4.

Student data may only be collected and used when meeting the educational needs of the child and as mandated by state and federal law. Student data shall not be disclosed to any party unless they are designated as the data owner (parent or student beyond the age of majority), an identified "School Official," or an "Authorized Representative' pursuant to federal FERPA guidelines acting in the best interests of the student's education. All record release requests shall be authorized by the District's Business Administrator (Custodian of Records). All student data requests shall be documented and archived as part of this policy.

When providing or delivering data to any stakeholder using any delivery mechanism, the West Orange Public Schools maintains compliance with the Family Educational Rights and Privacy Act (FERPA). For more information on FERPA, please visit the United States Department of Education's Family Educational Rights and Privacy Act (FERPA).

Personal Identifiable Information (PII) shall be disclosed only under the following conditions and employees shall be informed of such activity prior to release:

- Disaggregated Individual Student Data including but not limited to:
    - Allocation of state education funding;
    - Administering state assessments;
    - Calculating individual student growth;

- Aggregated (Summary and De-Identified) Student Data including but not limited to:
    - School and/or District Performance Reports;
    - Program evaluation and measurement;
    - School and District Improvement Plans;
    - Federal reporting/funding;
    - Public reporting.

Legal or Disciplinary Analysis – Student Personal Identifiable Information (PII) may be released to appropriate authorities to indicate the presence of activities that violate West Orange Board of Education policies and/or state/federal law. These requests shall be in response to documented policy incidents, legal discovery, or judiciary requests.

Network or Security Threats

All relevant data, protocol, logs and student information may be released as part of incident and breach analysis and remediation. The Department of Technology shall investigate and remediate possible network security threats by means of capture, logging, and examination of files, communications, and other traffic and transmissions on the WOBOE network including all student communications and network activities relevant to the incident or breach.

Student Data Requests

All requests to retrieve and share student data in digital or hardcopy must be submitted to the Department of Technology via the Business Administrator (Custodian of Records) or designee. Any litigation and legal requests require confirmation by the Chief School Administrator or the Business Administrator (Custodian of Records). Such requests shall include:

- Name and role of the requestor;
- Reason for the request, in accordance with the principles set forth in this and other related district Policies;
- Parental notification of the event (unless explicitly barred due to legal or disciplinary investigation) shall be made. In all circumstances, parents shall be notified when individual educational record requests are made that are not bound by legal constraints.

Student data shall not be intentionally shared with third parties outside of legally compliant (e.g. research, compliant third party provider operational contracts, federal and state reporting etc.) activities unless that data sharing is authorized by the parent, guardian, or student of majority. All student data requests shall be documented and stored as part of this policy.

Health Records

The maintenance and security of student health records shall be in accordance with N.J.A.C. 6A:32-7.4 and 6A:16-2.4. Student health records may be stored electronically, microfilm or in paper format and shall be maintained separately from other student records in a secure location accessible only by authorized personnel.

Employee Data Security Responsibilities

All West Orange Board of Education employees are responsible for to ensuring that all sensitive/confidential information in hard copy, microfilm or electronic form is secure in their work area at the end of the day and

when an employee expects to be gone for an extended period of time, the employee must adhere to the following best practices:

- Computer workstations must be locked when workspace is unoccupied;
- Computer workstations must be logged off completely down at the end of the work day;
- Any **Confidential** information must be removed from the desk and locked in a drawer when the desk is unoccupied;
- File cabinets containing **Confidential** information must be kept closed and locked when not in use;
- Keys used for access to **Confidential** information must not be left at an unattended desk or area;
- Passwords may not be left on sticky notes posted on or under a computer, nor should they be left written down in an accessible location;
- Printouts containing Confidential information should be immediately removed from the printer and stored in a secure location;
- The disposal of **Confidential** documents should be done in official shredder bins or placed in the locked confidential disposal bins;
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Training and Awareness of Data Privacy/ Security Policy and Procedures

The Department of Technology will conduct annual Privacy and Security Awareness trainings to all employees as part of an on-going training and awareness program. The training will be delivered in person/onsite and, when necessary, via online training modules.

Data Stewards, who may also be designated as trainers, will receive separate training that outlines additional roles and responsibilities as per their designated data systems and data management responsibilities. Data Stewards who manage systems that fall under the **Confidential** classification will be required to use 2-Factor Authentication.

The Privacy and Security Awareness training will include, but not be limited to, the following:

- Train employees on the importance of enabling and utilizing secure authentication, including the use of multi-factor authentication protocols;
- Train employees on how to identify different forms of social engineering attacks;
- Train employees on how to identify and properly store, transfer, archive and destroy sensitive information;
- Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.

Employees are required to annually sign an agreement form indicating that they have read, understood, and accept the terms and conditions outlined in the District's Data Privacy Security Policy, Internet Safety and Technology, Acceptable Use Policy, and all other relevant district policies adopted by the Board of Education.

In addition to delivering Privacy and Security Awareness training to all staff, the Technology Department will:

- Review and update the security awareness training program as needed, but at least annually, to address new technologies, threats, standards and business practice/requirements;
- Post and communicate updated privacy policies to employees, students, and parents via district website, District Communication Systems (School Messenger, Naviance, Email, and district social media);

- Define and make easily accessible processes for reporting privacy/security incidents and complaints (depending on the nature of the event, this may include reporting to the authorities, public, and/or individuals affected).

VPN (Virtual Private Network) Access

For the purpose of this document, remote access is defined as any faculty, staff, student, vendor, or any third party affiliate connecting to the WOBOE network using a VPN connection. A VPN is a secured private network connection built on top of a public network. It provides a secure encrypted connection, or tunnel, over the Internet between an individual computer/device and a private network such as the WOBOE district network. The use of VPN allows employees of the West Orange Public Schools to securely access our network from a remote location.

- All individuals and machines connecting remotely are subject to the district's Acceptable Use Policy (AUP);
- Users needing remote access to their work desktop machines, must use the VPN services provided, configured, and supported by the district's Technology Department;
- All district employees and any authorized third party using the VPN services must ensure that unauthorized users are not allowed access to the district's internal WOBOE network and its associated information/data;
- All individuals connecting remotely shall only connect to, or have access to, machines and resources they have permission and rights to use;
- All devices connecting remotely shall have current anti-virus software and all operating system and application updates and patches.

Approved Third-Party Services

Use of third party software and services that require the use/collection any district data, including students' Personal Identifiable Information (PII) within the scope of this policy, must be submitted to the Offices of the School Business Administrator and the Department Technology for review and approval by the Chief Data Steward(s).

The agreement with third-party providers shall prohibit Personal Identifiable Information (PII) in education records from being used for other purposes or redisclosed without the district's permission. Changing the terms of service of a contract or agreement without notice or documentation makes it difficult for a school or district to demonstrate direct control of the maintenance and use of the Personal Identifiable Information (PII). Therefore, the district agreement with third-party vendors will ensure that there is no unilateral modification provisions, ensuring that any changes in terms/policy are transparent and mutually agreed by both parties.

School service providers shall disclose in contracts and/or privacy policies what types of student Personal Identifiable Information (PII) are collected directly from students, and for what purposes this information is used or shared with third parties.

- Third-Party providers shall collect, use, or share student personally identifiable information only in accordance with the provisions of their privacy policies and contracts with the educational institutions they serve, or with the consent of students or parents as authorized by law, or as otherwise directed by the educational institution or required by law;

- Third-Party providers shall provide evidence that they have and enforce security policies and procedures designed to protect personal student information against risks such as unauthorized access or use, or unintended or inappropriate destruction, modification, or disclosure;

- Third-Party providers shall provide to the district documentation supporting that they follow industry standards and best practices for Cyber Security;

- Third-Party providers shall provide documentation that they have in place reasonable policies and procedures in the case of actual data breaches, including procedures to both notify educational institutions, and as appropriate, to coordinate with educational institutions to support their notification of affected individuals, students and families when there is a substantial risk of harm from the breach or a legal duty to provide notification.

A list of approved district software, mobile applications ("apps") and/or web-based tools that connect faculty and students with a third-party service provider will be posted on the district website. Faculty may only use the approved list of software to ensure the privacy and security student and employee data in the district.

All new software and apps must be submitted by district administration to the Department of Technology. The software or app will be reviewed by a committee and vetted to ensure that it meets standards set forth in this policy. Once the software is approved, it shall be posted on the district website with a link to the vendor's user agreement and data security policy.

Policy Violation

Violation of this policy may incur the same types of disciplinary measures and consequences as violations of other District policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting of a Student Code of Conduct violation.

Violation of this policy may also result in termination of contracts or commitments to vendors and other affiliates. Legal action may be pursued where appropriate.

Key Words

References:

FERPA

https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Legal References:

NJAC 6A:32-7.4
NJAC 6A:16-2.4