Nassau County School District

Data Classification and Handling Policy

Nassau District Schools

"character, conscience, competence"

Nassau County School District
1201 Atlantic Avenue
Fernandina Beach, FL 32034

Purpose

The purpose of this policy is to establish a framework for classifying and handling district data based on its level of sensitivity, value and criticality to the district as required by the district's Information Security Plan and Network Procedures. Classification of data aids in determining baseline security controls for the protection of data.

Scope

This policy applies to all district employees who access, process, or store sensitive district data.

Definitions and Responsibilities

Confidential Data- Data classified as confidential according to the data classification scheme defined in this document. This term is often used interchangeably with sensitive data.

Data Owner- An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department or school.

- Data Owners are responsible for having an understanding of legal and contractual obligations surrounding information assets within their functional areas. For example, the Family Educational Rights and Privacy Act ("FERPA") dictates requirements related to the handling of student information.
- A Data Owner is accountable for who has access to information assets within their functional areas.
- A Data Owner may decide to review and authorize each access request individually or may define a set of rules that determine who is eligible for access based on business function, support role, etc. Access must be granted based on the principles of least privilege as well as separation of duties. For example, a simple rule may be that all students are permitted access to their own transcripts or all staff members are permitted access to their own health benefits information. A Data Custodian should document these rules in a manner that allows little or no room for interpretation.

Data Custodian- Employee of the district who has administrative and/or operational responsibility over information assets and must follow all appropriate and related security guidelines to ensure the protection of sensitive data and intellectual property residing on systems for which they have accountability.

- Understanding and documenting how information assets are being stored, processed and transmitted is the first step toward safeguarding that data. Without this knowledge, it is difficult to implement or validate safeguards in an effective manner.
- Data Custodians are responsible for provisioning and deprovisioning access based on criteria established by the appropriate Data Owner.

- Data Custodians need to have a thorough understanding of security risks impacting their information assets. For example, storing or transmitting sensitive data in an unencrypted form is a security risk. Protecting access to data using a weak password and/or not patching vulnerabilities in a system or application are both examples of security risks.

Data User- Any employee, contractor, or third-party provider of the district who is authorized to access the district's information systems and/or assets.

- Data Users are also required to follow all specific policies, guidelines, and procedures established by departments or schools with which they are associated and that have provided them with access privileges.

Institutional Data- All data owned or licensed by the district.

Information Assets- Definable pieces of information in any form, recorded or stored on any media, that is recognized as "valuable" to the district.

Non-public Information- Any information that is classified as Internal/Private Information according to the data classification scheme defined in this document.

Sensitive Data - Term that typically represents data classified as confidential according to the data classification scheme defined in this document.

Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the district should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity tiers:

Tier 1-Confidential Data

Data should be classified as Confidential when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the district or its affiliates. Examples of Confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied.

Access to Confidential data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the district who require such access in order to perform their job ("need-to-know"). Access to Confidential data must be individually requested and then authorized by the Data Owner who is responsible for the data.

Tier 1 Confidential data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the district should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of Confidential/Restricted data include official student grades, social security numbers, and individuals' health information.

Tier 2-Internal/Private Data

Data should be classified as Internal/Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the district or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public data should be treated as Internal/Private data. A reasonable level of security controls should be applied to internal data.

Access to Internal/Private data must be requested from, and authorized by, the Data Owner who is responsible for the data. Access to Internal/Private data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department.

Internal/Private Data is moderately sensitive in nature. Often, Tier 2 Internal/Private data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the district should this information not be available when needed is typically moderate. Examples of Internal/Private data include official district records such as financial reports, human resources information, instructional software reports, and unofficial student records.

Tier 3-Public Data

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the district and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public data should be protected. The appropriate Data Owner must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should Tier 3 Public data not be available is typically low, inconvenient but not debilitating. Examples of Public data include directory information, course information, and research publications.

Data Collections

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student's name, address, and social security number, the data collection should be classified as Confidential even though the student's name and address may be considered Public information.

Determining Classification

The goal of information security, as stated in the district's Information Security Plan and Network Procedures, is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to the district if confidentiality, integrity or availability of the data is compromised.

Potential Impact			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Potential Impact			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Predefined Types of Confidential/Restricted Information Assets
Based upon state, federal, and contractual requirements that Nassau County School District is bound by, the following information assets have been predefined as Level 1 or Level 2 data and must be protected:

Personally Identifiable Education Records-Covered under FERPA
Personally Identifiable Education Records are defined as any education records that contain one or more of the following personal identifiers:

- Student ID Number
- Grades, GPA, Credits Enrolled
- Social Security Number • Race/Gender
- A list of personal characteristics or any other information that would make the student's identity easily traceable

Personally Financial Identifiable Information (PIFI) - Covered under GLBA
For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- Date of Birth
- Financial account number in combination with a security code, access code or password that would permit access to the account

Protected Health Information (PHI) - Covered under HIPAA

PHI is defined as any “individually identifiable” information that is stored by a Covered Entity, and related to one or more of the following:

- Past, present or future physical or mental health condition of an individual.
- Provision of health care to an individual.
- Past, present or future payment for the provision of health care to an individual.

PHI is considered “individually identifiable” if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
- Telephone/Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristic that could identify an individual

If the health information does not contain one of the above referenced identifiers and there is no reasonable basis to believe that the information can be used to identify an individual, it is not considered “individually identifiable” and; as a result, would not be considered PHI.

Data Handling Requirements

For each classification, several data handling requirements are defined to appropriately safeguard the information. It’s important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability.

The following table defines required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	**Data Classification**		
	Tier 3-Public	**Tier 2-Internal**	**Tier 1-Confidential**
Copying/Printing (applies to both paper and electronic forms)	No restrictions	Data should only be printed when there is a legitimate need Copies must be limited to individuals with a need to know. Data should not be left unattended on a printer/fax. May be sent via interoffice mail.	Data should only be printed when there is a legitimate need. Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement. Data should not be left unattended on a printer/fax. Must be sent via envelope marked “Confidential”.
Network Security	May reside on a public network. Protection with a firewall recommended. IDS/IPS protection recommended. Protection only with router ACLs acceptable.	Protection with a network firewall required. IDS/IPS protection required. Protection with router ACLs optional. Servers hosting the data should not be visible to entire Internet. May be in a shared network server subnet with a common firewall ruleset for the set of servers.	Protection with a network firewall using "default deny" ruleset required. IDS/IPS protection required. Protection with router ACLs optional. Servers hosting the data cannot be visible to the entire Internet, nor to subnets like the guest wireless networks. Must have a firewall ruleset dedicated to the system. The firewall ruleset should be reviewed periodically.

Security Control Category	Data Classification		
	Tier 3-Public	Tier 2-Internal	Tier 1-Confidential
System Security	Must follow general best practices for system management and security. Host-based software firewall recommended.	Must follow district-specific and OS-specific best practices for system management and security. Host-based software firewall required. Host-based software IDS/IPS recommended.	Must follow district-specific and OS-specific best practices for system management and security. Host-based software firewall required. Host-based software IDS/IPS recommended.
Virtual Environments	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines. Cannot share the same virtual host environment with guest virtual servers of other security classifications.
Physical Security	System must be locked or logged out when unattended. Host-based software firewall recommended.	System must be locked or logged out when unattended. Hosted in a secure location required; a Secure Data Center is recommended.	System must be locked or logged out when unattended. Hosted in a Secure Data Center required. Physical access must be monitored, logged, and limited to authorized individuals 24x7.

Security Control Category	**Data Classification**		
	Tier 3-Public	**Tier 2-Internal**	**Tier 1-Confidential**
Remote Access to systems hosting the data	No restrictions.	Access restricted to local network or VPN. Remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the Internet.	Restricted to local network or secure VPN group. Unsupervised remote access by third party for technical support not allowed. Two-factor authentication recommended.
Data Storage	Storage on a secure server recommended. Storage in a secure Data Center recommended.	Storage on a secure server recommended. Storage in a secure Data Center recommended. Should not store on an individual's workstation or a mobile device.	Storage on a secure server required. Storage in Secure Data Center required. Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption. Encryption on portable backup media required. Paper/hard copy: do not leave unattended where others may see it; store in a secure location.
Transmission	No restrictions.	No requirements.	Encryption required (for example, via SSL or secure file transfer protocols). Cannot

			transmit via e-mail unless encrypted and secured with a digital signature.
Security Control Category	**Data Classification**		
	Tier 3-Public	**Tier 2-Internal**	**Tier 1-Confidential**
Backup/Disaster Recovery	Backups required; daily backups recommended.	Daily backups required. Off-site storage recommended.	Daily backups required. Off-site storage in a secure location required.
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper,etc.)	No restrictions.	Recycle reports; Wipe/erase media.	Shred reports. Destruction of electronic media.
Training	General security awareness training recommended.	General security awareness training required. Data security training required.	General security awareness training Required. Data security training required. Applicable policy and regulation training required.
Auditing	Not needed.	Logins.	Logins, access and, changes.
Mobile Devices	Password protection recommended, locked when not in use.	Password protected, locked when not in use.	Password protected, locked when not in use. Encryption used for Level 3 data.