Norfolk Public Schools
The cornerstone of a proudly diverse community

Norfolk Public Schools Data Governance Plan: Addressing data governance Checklist Questions

Introduction

Norfolk Public Schools (NPS) is dedicated to ensuring the safety, integrity, and proper use of all students, staff, and district data. This Data Governance Plan has been developed to address the questions outlined in the data governance framework checklist, focusing on data management practices, compliance, accountability, and data privacy. By implementing a robust data governance framework, NPS aims to protect sensitive information, facilitate data-driven decision-making, and promote transparency and ethical use of data across the district.

Checklist Questions and Responses

1. What Types of Data Are Collected?

- **Student Data**: This includes personally identifiable information (PII), academic records, health information, behavioral data, and attendance records.
- **Staff Data**: Employment records, payroll information, certifications, evaluations, and personal information are collected for effective workforce management.
- **Operational Data**: Financial records, budget information, facility usage, transportation details, and other internal records are collected to ensure efficient district management.
- **Third-Party Data**: Data collected and shared with vendors and third-party providers, such as learning management systems, assessment tools, and educational technology solutions, must comply with data privacy requirements.

2. Who Is Responsible for Data Management?

- **Data Governance Team**: NPS has established a Data Governance Team responsible for overseeing the collection, usage, storage, and sharing of data. The team includes representatives from IT, legal, curriculum, and other departments.
- **Data Stewards**: Specific data stewards have been assigned different types of data (e.g., student data, staff data, financial data). These individuals ensure compliance with data governance policies and procedures.
- **Cybersecurity Team**: A dedicated cybersecurity team oversees data security, privacy measures, and incident response related to data breaches.

- **Data Governance Body**: Establish a formal data governance body to oversee strategic data initiatives, coordinate between departments, and ensure alignment with district goals.
- **Executive Sponsorship**: Ensure that NPS leadership actively supports and sponsors data governance initiatives, allocating necessary resources and communicating the value of data governance across the district.

3. What Policies Govern Data Use?

- **Data Governance Policy**: A comprehensive Data Governance Policy has been implemented to define roles, responsibilities, and procedures for data handling, including data collection, storage, access, sharing, and destruction.
- **Acceptable Use Policy (AUP)**: The AUP has been updated to include guidance on the use of data by students, staff, and third parties, emphasizing responsible data usage, privacy, and ethical considerations.
- **Data Privacy Policy**: This policy outlines how student and staff data is protected, including measures to prevent unauthorized access, data breaches, and misuse. It also covers compliance with FERPA, COPPA, and other applicable regulations.
- **Third-Party Data Sharing Policy**: A specific policy governs the sharing of data with vendors, ensuring they comply with district standards for data privacy, security, and ethical use.
- **Policy Update Cycle**: Formalize a schedule for regular review and updates of all data-related policies to maintain alignment with best practices and regulatory changes.
- **Purpose-Driven Governance**: Develop clear purpose statements for data governance activities, defining success metrics, and illustrating how these initiatives support educational outcomes and innovation.

4. How Is Data Security Ensured?

- **Encryption**: All data in transit for Office 365 is encrypted using advanced encryption protocols, such as AES-256, to protect sensitive information.
- **Access Controls**: Role-based access control (RBAC) is in place to ensure that only authorized personnel have access to specific data. Multi-factor authentication (MFA) is required for accessing critical systems.
- **Data Masking**: Data masking techniques are used to protect sensitive information during testing and development activities, ensuring that real data is not exposed in non-production environments.
- **Regular Security Audits**: Annual security audits by third-party experts, as well as internal audits conducted quarterly, help identify vulnerabilities and ensure compliance with district policies.
- **Proactive Security Processes**: Document proactive processes, including setting standards before data collection, to prevent security issues from arising.

- **Automation**: Utilize automation tools to streamline data governance tasks, including data security and access management, to reduce manual errors and improve efficiency.

5. How Is Data Quality Maintained?

- **Data Validation**: Automated data validation processes are implemented to ensure data accuracy during data entry, reducing the likelihood of errors.
- **Data Cleansing**: Regular data cleansing procedures are performed to eliminate duplicates, correct inaccuracies, and update outdated information.
- **Data Quality Monitoring**: Data quality metrics are tracked to monitor completeness, accuracy, consistency, and timeliness. Data stewards regularly review these metrics to maintain high data quality standards.
- **Data Quality Documentation**: Maintain comprehensive documentation of data quality processes to ensure consistency and facilitate training for new staff.
- **Empowering Data Stewards**: Encourage data stewards to actively share knowledge and best practices, promoting a collaborative environment that enhances data quality and governance.

6. How Are Data Privacy and Compliance Maintained?

- **FERPA, COPPA, and GDPR Compliance**: All data handling practices comply with federal and state regulations, including FERPA, COPPA, and GDPR, ensuring that student and staff data privacy is prioritized.
- **Vendor Compliance Audits**: Vendors are required to undergo compliance checks before engagement and must agree to periodic audits to verify continued compliance with district privacy standards.
- **Staff Training**: Staff members receive regular training on data privacy laws, compliance requirements, and best practices for protecting sensitive information. Training is conducted annually, with refresher courses offered every six months.
- **Data Breach Response**: Develop a detailed response plan for handling data breaches, including steps for mitigation, notification, and reporting.

7. How Is Data Access Monitored and Controlled?

- **Access Control Lists (ACLs)**: ACLs are used to control access to sensitive data based on job roles and responsibilities. Permissions are reviewed regularly to ensure only authorized individuals have access.
- **Logging and Monitoring**: All access to data is logged, and logs are regularly reviewed to detect unauthorized access attempts. The Security Information and Event Management (SIEM) system helps in real-time monitoring and alerts.
- **Third-Party Access**: Access to data by third-party vendors is restricted based on contractual agreements. Vendors must comply with district security protocols, and their access is monitored continuously.

- **Access Control Documentation**: Ensure that all access control policies and procedures are fully documented to provide clarity and consistency in managing data access.
- **Iterative Processes**: Adopt a flexible and iterative approach to access control, allowing adjustments based on changes in district requirements and emerging technologies.

8. How Is Data Retention Managed?

- **Data Retention Policy**: NPS has implemented a Data Retention Policy that defines how long different types of data must be retained, ensuring compliance with regulatory requirements and district needs.
- **Automated Deletion**: Automated data deletion processes are in place for data that has reached the end of its retention period. This helps ensure that outdated information is removed, reducing the risk of unnecessary data exposure.
- **Archiving**: Critical data that needs to be retained for historical or legal purposes is archived securely, with access controls in place to prevent unauthorized retrieval.
- **Data Lifecycle Management**: Establish a clear data lifecycle management process that tracks data from creation to deletion, ensuring consistent and compliant handling throughout its lifecycle.

9. How Are Stakeholders Trained in Data Governance?

- **Staff Training Programs**: All staff members are trained in data governance policies and procedures, including data privacy, security, quality, and compliance. Training includes workshops, online modules, and scenario-based exercises.
- **Student and Parent Resources**: Students and parents are provided with resources that explain data privacy and how their information is used by the district. Informational guides and workshops are made available to build awareness and trust.
- **Training for Data Stewards**: Data stewards receive specialized training on data management, monitoring, and compliance to ensure that they are fully equipped to manage their assigned data effectively.
- **Ongoing Stakeholder Engagement**: Implement regular engagement activities for stakeholders, including feedback mechanisms to continually refine and improve data governance processes.
- **Define Clear Objectives**: Articulate specific, measurable goals for data governance efforts, demonstrating their impact on educational outcomes and operational efficiency.

Action Plan

- **Immediate Actions (0-3 Months)**:
  - Finalize and distribute the Data Governance Policy for acknowledgment by all staff.

    - Train data stewards in their roles and responsibilities related to data governance.
    - Initiate vendor compliance checks to verify adherence to data privacy standards.
- **Mid-Term Actions (3-6 Months)**:
    - Implement automated data validation and cleansing processes to maintain data quality.
    - Conduct training workshops for staff on data privacy, security, and acceptable use policies.
    - Set up automated data deletion processes for data at the end of its retention period.
- **Long-Term Actions (6-12 Months)**:
    - Perform a comprehensive security audit and adjust policies based on audit findings.
    - Establish ongoing data governance training programs for staff, students, and parents.
    - Develop a data archiving system for secure storage of critical historical data.

Regular Updates and Revisions

NPS is committed to keeping data governance policies and procedures current with evolving best practices, regulatory requirements, and technology advancements. The Data Governance Team will conduct periodic reviews and make necessary updates to ensure continued compliance and effectiveness.

Conclusion

The Norfolk Public Schools Data Governance Plan provides a comprehensive framework to ensure the security, privacy, and ethical use of student, staff, and district data. By addressing data governance needs through policies, procedures, training, and continuous improvement, NPS is committed to protecting sensitive information, promoting responsible data use, and empowering stakeholders to make informed decisions. For more information, please contact the Data Governance Team or visit the Data Privacy section on our website.