Indicators of Digital Readiness

Indicator	**Data Security and Privacy**
Theme	**Technology Support and Services**
Priority Level	**P1**
Organizational Level	**District**

Description of the Indicator

Districts need to take reasonable steps to ensure the security of data systems in addition to the integrity and privacy of collected data. Policies and procedures should be developed to ensure the data systems they host are secure and data systems that they interact with have sufficient breach notification and strong privacy policies. Policies should also provide role-specific guidance to staff to safeguard data and ensure best practices are followed when accessing, collecting, storing and/or using data.

Why is this indicator important?

As Districts collect more information about our students and staff it is vital that the data be kept private and secure. This is not only a regulatory requirement, but part of the essential trust between a District and their students, parents and staff.

Indicator Rubric

Insufficient Evidence of Implementation **(0 Points)**	● The district has not started the process of identifying/classifying data and assigning data stewards to systems ● There are no policies or the district is in the process of drafting policies and procedures ● There is no existing process for incident responses ● Districts have not started dialogue with Third-Party vendors regarding policies and procedures to protect students and faculty data
Foundational Stage of Implementation **(3 Points)**	● The district started the process of identifying and classifying data in their systems and is in the process of assigning roles and data stewards for all systems ● Policies and procedures are being created or revised ● The district has initiated the conversation with Third-Party vendors to address the need to align data security/privacy policies and procedures
Achieving Success in Implementation **(6 Points)**	● District data has been identified, classified, and assigned to the right users and has been placed under the guidance of designated data stewards ● Policies and procedures designed to protect student and faculty data have been Board approved and communicated to students, faculty, and parents ● The district is developing policies and procedures with Third-Party vendors that follow best practices and industry standards to protect student data and privacy ● Incident Response Plans are in the development stage
Exemplary Success in Implementation **(9 Points)**	● The district has taken the necessary steps to protect the integrity and privacy of collected data in all systems ● Data has been identified, classified, and assigned to the right users and has been placed under the guidance of designated data stewards ● Policies and procedures designed to protect student and faculty data have been Board approved and communicated to students, faculty, and parents ● The district has established third-party data sharing/storage policies with

	most or all Third-Party vendors ● Incident Response Plan has been created and shared with responsible parties ● Policies and procedures are scheduled for ongoing review and a plan is in place to communicate policy changes to students, faculty, and parents via multiple communication channels: district Website, email, social media, and or communication systems

Who in the school/district should lead and be involved with this indicator?

Superintendent, Business Administrator, Technology Coordinator/Director of Technology/CIO, Director of Curriculum, other staff as deemed necessary by the principal members of the indicator.

How to execute the indicator

- Maintain a Board-approved Data Privacy and Security Policy for student and staff data placed prominently on the district's or school's website.
- Completed Data Privacy and Security Policy should include the following components:
    - District's/School's Data Governance Charter
    - Classification/Definitions of types of data collected or available.
    - Data system inventory
        - Inventory of hosted and subscribed data systems and the type of data that is stored on each data system. This inventory should also contain 3rd party systems and plugins what have access to district/school data systems. The inventory should contain a copy or link to the data systems terms of service and privacy policy with a date of review.
        - A version of this inventory should be made public and accessible from the district/school website for parents and updated as systems are on-boarded/off-boarded.
    - Data stewardship by system and/or data type
    - Data accessibility matrix based on classification/role
    - Responsible-use guidelines for staff and students regarding:
        - Accessing;
        - Collecting;
        - Storing;
        - Maintaining/Updating;
        - Using;
        - Sharing/Presenting;
        - Retaining; and
        - Destroying Data

- Third-party data sharing/storage policy
  When is data shared or stored with outside parties/vendors? What are the requirements?
- List of vendors and contractors that have access to district/school networks and systems and for what purpose.
- An incident response/breach notification plan with appropriate contacts
- Related policies, laws and regulations

- Review/update policy at least once per year.

Optional Checklist for Guidance:

Milestone/Component	Completed
Data has been identified and classified by type	
Data access has been assigned by role (access matrix)	
Data stewards have been designated by type/system	
Responsible-use Policies have been developed for staff and students	
Third-party data sharing/storage policy included	
Incident response plan included	
Policy is reviewed at least once per year	
Policy has not been board approved and/or posted on District website	

Evidence to submit for successful execution of this action

- Completed board-approved data security and privacy policy
- Public version of data system inventory/matrix for parents

Resources schools can use to complete this action successfully

- Privacy Technical Assistance Center (PTAC) Toolkit
- COSN Protecting Privacy
- Student Privacy and Data Security Toolkit for Service Providers
- FERPA/PPRA Information

- COPPA
- Example Policy

Certified Schools Exemplars

1. **Hackensack Middle School, Hackensack Public Schools, 2018 Bronze Certified**

   The District has made Data Privacy a major focus over the last year and as such integrated it into all PD that may involve online resources or using data. A District Data Privacy Initiative section is available on the website and provides resources for parents regarding our Data privacy and security practices as well as currently approved resources. A separate staff-only version is available through our Digital Learning Center and includes an interactive version of our Data Privacy and Security policy with links to forms, resources and training videos. We have also established a thorough review process for all applications and third-party vendors that may use District data. Vendors who do not meet the requirements or do not provide information regarding their data privacy and security practices and policies are not approved.

2. **Memorial School, Old Bridge Township Public Schools, 2018 Bronze Certified**

   Data from these applications from these systems is collected and shared via secure One Drive. District Administration is able to solicit and receive data from all sources. Utilizing Soar the Score reports, Achieve 3000 and iReady reports, allows district personnel to assess multiple sources for a given student, coupled with historical interventions, programs, attendance, and assignment-level grades.

   Shared but secure resources provide staff with the ability to view and compare assessment information longitudinally, as well as demographically.

   The district utilizes Realtime Student Information system and it is the heart of student information. The district has a system of data connectors that provide us with Active Directory, Microsoft account creation, library automation system accounts, and food services accounts. These data points are synchronized daily. This assures us that all student information is consistent over multiple educational and service-based applications.

   Using data collected from our core applications combined with external learning applications, we can provide critical feedback to the staff through data analysis. Most reports and widgets are “drill-down” in nature, where the staff can view high level information and quickly “drill-down” to see granular details of student information.

   The district and a small team of stakeholders has been working with our Student Information System vendor, Realtime, to integrate Microsoft ClassNotebook with Realtime Gradebook. This has been an on-going project which we expect to see come to fruition in August, 2018. Integration of these two applications will allow teachers to enter a grade in ClassNotebook and have it automatically “synch” to Realtime Gradebook, thus eliminating duplication of effort.

   In addition, the district also utilizes a “student synch” application which automatically synchs student accounts and updates student accounts for use on our network.

   Software applications, such as iReady, Achieve 3000, Frontline applications, etc., all synch nightly with our Realtime student information system.

   All users have unique account credentials for accessing computer systems via Microsoft Active Directory Group Policy. Users are limited access based on the permissions assigned to their group (I.e., students see less than teachers; no software downloads, etc.). Upon unsuccessful login, accounts are locked after three attempts and are an only be reset by technology staff. Upon termination of employment, accounts are locked. Certain applications require double authentication upon login as an extra measure of security (Microsoft, Realtime, etc.). Users are prompted via system notification to reset their passwords every 90 days. Guidelines are provided to all staff to choose strong passwords. These guidelines come to staff via email notification as well as in faculty meetings several times a year.