Indicators of Digital Readiness

Indicator	**Staff Awareness**
Theme	**Technology Support Services**
Priority Level	**P2**
Organizational Level	**District**

Description of the Indicator

There is a policy or program in place to educate staff (at least annually and/or during the onboarding process for new staff) on the District's Data and Privacy vision and all relevant policies, procedures and practices. Changes or additions to policies or State and Federal laws that may impact data governance are disseminated as quickly as possible to staff either in writing or via electronic format.

Why is this indicator important?

Educating staff on appropriate/responsible data practices, procedures, and policies will ensure compliance with State and Federal requirements. Additionally, this will improve data quality and access to relevant, timely data for instruction while also safeguarding student and staff privacy.

Indicator Rubric

Insufficient Evidence of Implementation **(0 Points)**	● Nothing is currently implemented ● Policies, procedures and best practices exist but there is currently no concerted effort beyond distribution of policy/procedures to raise awareness or train staff on how to effectively use data
Foundational Stage of Implementation **(2 Points)**	● Staff are made aware of policies once or periodically, especially when issues arise, but no formal proactive approach to promoting security/privacy is in place
Achieving Success in Implementation **(4 Points)**	● Staff are made aware of policies, procedures and best practices at least annually or as they are hired, but training is very general in nature and there is no school or district-wide emphasis on privacy or security
Exemplary Success in Implementation **(6 Points)**	● District-wide Privacy Program/Initiative is in place ● Staff are thoroughly trained on data privacy and security policies, procedures and practices as it pertains to their role and data privacy awareness is integrated into all District educational programs ● Staff commit to cognizantly maintaining data privacy utilizing knowledge and resources received through trainings and continued support ● All staff are expected to model best practices when handling sensitive information

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

- District Data Governance Team and/or District Technology/Digital Learning Committee
- Professional Development Department/Committee
- Human Resources where applicable
- Building Administrators

How to execute the indicator

Develop a plan that includes the following:

- Raising awareness through real-world examples to demonstrate to staff the importance of protecting data and/or following best practices.

- Training all employees and temporary/contracted employees.
- Integrate data security training within the context of broader employee education efforts.
- Tailoring training courses to employee roles to ensure relevant data handling/management practices are being shared.
- Raising awareness of protocols related to breach detection and escalation.
- Including data security messages in employee communications channels where appropriate.
- Creating a culture of security in the organization by having administrators model best practices.

Training should include the following components:

- Risk assessment including the identification of system threats and vulnerabilities.
- Physical security (e.g., locked doors and windows), desktop security (e.g., password protected computers, mobile device security (e.g., no sensitive data on easily misplaced storage media), and network security (e.g., secure data exchange).
- Access controls including how to password protect files, encrypt transmissions and files, and authenticate users.
- Good practices related to the use of email, software/applications, and the internet.
- Train staff in having awareness of phishing, hoaxes, malware, viruses, worms, spyware and to alert IT department.
- Provide appropriate procedures for those who require remote access to data and systems.
- Data backup and disaster recovery plans are in place for appropriate personnel.

Other Recommended Actions:

- Create a Data Protection Pledge for staff and/or students in an effort to raise awareness.
- Gather all relevant policies and resources in a single, easily accessible location for all staff.
- Hang Privacy-related fliers in visible locations within offices and schools and keep handouts/information pamphlets available in offices and staff lounges. Share material via email and online on District and/or School websites as well.
- Create District Data Awareness section/page for parents on the District/School Website that is visible on or easily accessible from the homepage (or parent page) and highlights the steps being taken by the District to protect data privacy with links to any relevant resources.
- Create talking-points for teachers/administrators to share at “back-to-school” nights and other parent events.
- Optional: Engage local media to raise awareness of the District’s or School’s Data Protection campaign/program.

Evidence to submit for successful execution of this action

- Action plan
- Training course documentation/agenda and sign-ins

- Sample signed policy and related materials
- Link to district/school webpage with resources

Resources schools can use to complete this action successfully

- Data Security and Management Training: Best Practice Considerations
- Choose Privacy Week
- Resources for talking points and other content
- Safe Schools Training on data privacy and digital security (or other similar type program)
- Google Digital Safety Center
- ACES- Digital Safety for Schools
- USDOE- Protecting Student Privacy
- Be Internet Awesome

Certified Schools Exemplars

1. **Linden High School, Linden Public Schools, 2018 Bronze Certified**

   The Linden School District has taken reasonable steps to ensure the security of data systems, as well as to govern and protect the integrity and privacy of all the data that is collected. The district's policies and procedures have been developed to ensure our data systems both onsite and those which are in the cloud, have sufficient breach notification and strong privacy policies. As we collect more information about our students and staff, it is our duty and responsibility that this data is kept private and secure. Staff training occurs throughout the year both formally and informally. This training includes new staff orientation, acceptable use policies, using district-provided technology, and other training as-needed. Workshops are provided not only during the school year, but during the summer, as well. Technology newsletters are distributed twice per year, which includes updates to procedures and policies. LPS staff is also updated through emails, and announcements in our LMS and District website.

2. **North Boulevard Elementary School, Pequannock Township School District, 2018 Bronze Certified**

   The Pequannock Township School District implements a comprehensive digital privacy and security training program, aligned with district policy and as it pertains to the staff member. All Pequannock staff members are expected to implement the safety and security skills gained during training in their ongoing use of technology systems and most go to lengths to report security concerns. Staff maintain best practice both in and out of school, including outside school hours and on their own private systems, and defer to security or IT when a question arises. Policy and other changes are disseminated via school administrators within 3 days of each board meeting implementing the change. The staff of the Pequannock Township District are continually made aware of the importance of network security and integrate the ideas of network/internet security to their students.

3. **G. Harold Antrim Elementary School, Point Pleasant Beach School District, 2018 Bronze Certified**

   The G. Harold Antrim Elementary School is committed to making sure students and staff are well-trained and aware of proper use of devices. Multiple trainings, professional development opportunities, and professional discussions are centered around productive and positives uses of technology. Information regarding policies and procedures are posted on the school's website. In addition, teachers have access to information via our student information system (Genesis). This provides teachers and staff with pertinent information regarding their students and their programs.

4. **Robert Menendez Elementary/PS #3, West New York, 2018 Bronze Certified**

   The West New York school district recognizes the importance of securing its data and systems from internal and external threats. Most successful cyber incidents and security breaches are the result of human error. In order to meet compliance

and mitigate risk, the District has implemented a Security Awareness program to ensure all users are well educated regarding best information security practices. The District initiated the program by training all Administrators, Faculty and Staff during several presentations at the beginning of the school year. Central Office personnel and new faculty and staff were trained at subsequent training events. The District also uses SafeSchools for online training such as FERPA. As part of the initiative and ensuring that all staff maintain a high level of “constant” awareness, the District purchased additional online training from Knowbe4. They are a leading security awareness platform that allows the delivery of small bite training videos and targeted phishing campaigns to assess staff awareness.