Data Security and Privacy Training

Best Practices for Protecting Data

Data Inventory

Address key questions with a data inventory: What systems do we have? What data do they store? What reports and exports are available? Who are the users?

Designate a Privacy Officer

School districts should determine who is responsible for data management and privacy issues including educating of staff, management and delivery of data, and maintaining agreements and contracts.

De-identify Data

De-identify data used in analysis, research and presentations using random identifiers. Be careful not to indirectly identify students in small subgroups. Use aggregated data where applicable.

Passwords

Employ password protection strategies:

- Use unique passwords and change them frequently.
- Do not write down passwords, and disable "Remember Password" functions in browsers.
- Use strong passwords. Mix upper and lower case letters, numbers and symbols where possible. Use a passphrase to make passwords easy to remember.
- Avoid weak passwords. Examples include your login, common words and passwords that contain easily accessible information and sequences of only numbers and letters.

Email

Consider security and privacy issues related to everyday use of email. Senders no longer control information after it is emailed. Do not send personal and sensitive information in email bodies or attachments.

Workstation and File Security

Lock workstations when not in use. Follow district policy and procedure on electronic and physical file storage locations. Also follow district policy on using secure methods to transfer files (such as network drives for internal transfers and SFTP applications for external transfers).

Created by the NYS RICs Data Security and Privacy Project Team

Data Security and Privacy Training

Best Practices for Protecting Data

Mobile Computing Devices - MCDs

Implement MCD policies and inventory data and equipment. Policy should include proper use and protection of data on MCD's, breach notification policy and directions for employees in the event of a data breach.

Technical Issues

Assess technical procedures including perimeter defenses, LAN and WAN management, vulnerability, encryption, patch and virus management, software updates, and crisis management.

Data Access and Permissions

Implement policy and procedure regarding access to data and user account management so that data access is strictly on a "need to know" basis. Best practices include reviewing staff duties annually, adjusting permissions when duties change, deactivating form employee accounts, eliminating generic accounts and reviewing audit logs.

Verbal Communication

Remember that verbal communication issues are an important consideration. Conversations that include personal and sensitive information can be easily overheard. Don't share sensitive information with unauthorized people and while socializing.

Paper Copies

Keep paper copies secure. Consider whether printouts are really needed. Promptly retrieve printed copies, and store copies securely.

Data Destruction

Destroy documents and files when no longer needed and minimize the amount of data retained. Data should be removed in a way that renders it unreadable (for paper records) or irretrievable (for digital records). Require third parties receiving PII under the FERPA School Official Exception to destroy it when the relationship is terminated or when no longer needed (whichever comes first). Also require third parties receiving PII under other FERPA Exceptions to destroy it when no longer needed.

NEW YORK STATE
REGIONAL INFORMATION CENTERS

Created by the NYS RICs Data Security and Privacy Project Team