SAU3 Data Governance Manual

Due to the new NH HB1612 law we are now required to follow the state guidelines regarding student and staff data privacy and security.

Important Main Points

Must Follow State/Federal Laws, and District Policies/Procedures

- All persons who have access to district data are required to follow state and federal law, district policies and procedures, and other rules created to protect the information.

- For a list of Policies Laws and Guidelines please see the SAU3 website.

Accessing Data from Outside the District

- If permission is given, the data may be accessed with appropriate security. When users access confidential or critical data from a remote location, the user must take precautions to ensure that the confidential or critical data is not downloaded, copied or otherwise used in a manner that would compromise the security and confidentiality of the information.

Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of PII or Confidential Information.
- Sharing your user IDs or passwords with others (exception for authorized technology staff for the purpose of support)
- Applying for a user ID under false pretenses or using another person's ID or password.
- Unauthorized use of an authorized password to invade student or staff privacy by examining records or information for which there has been no request for review.
- Installation or use of unlicensed software or software not approved for district technological systems.

Do Not Share Passwords

- Users will be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall not be shared.

Use of Software or Websites

- However, **before** any online service or application is purchased or used to collect or store confidential or critical information, including confidential information regarding students or staff, the Information Security Officer (ISO - IT Dept.) or designee must approve the use of the service or application and verify that it meets the requirements of the law and School Board policy and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

- Memorandums of understanding (MOU), contracts, terms of use and privacy policy for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO **prior to initiation**.

New Resource Acquisition

- The Berlin Public School District has an established process for vetting new digital resources. Staff are required to complete a helpdesk ticket, to ensure that all new resources meet business and/or instructional need as well as security requirements. The IT department will notify the staff member if the new resource meets the requirements and if it can be used.
- This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.
- Under no circumstances can staff act as a parental agent when creating student accounts for online resources; resources requiring this permission must be approved at the district level.

New Resource Acquisition Continued

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO **prior to initiation**. Staff should speak with their building Technology Integrator before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.

Observing Security Protections

- All individuals using confidential and critical information will strictly observe protections put into place by the district including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information in a confidential and secure manner.

- Confidential paper records will be destroyed using methods that render them unreadable, such as shredding. Confidential digital records will be destroyed using methods that render the record unretrievable.

File Transmission Practices

- Staff are responsible for securing sensitive data for transmission through email or other channels. Staff should not transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval. When possible, staff should de-identify or redact any PII or confidential information prior to transmission (see Appendix F: Securing Data at Rest and Transit).

- Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be reviewed and approved by the Superintendent or designee.