Data Breach Prevention and Response Plan

The District's Cybersecurity Coordinator is responsible for annually reviewing this plan and updating the guidelines as needed.

Security breach prevention

Maintain and update the breach response team contact list: Check that the contact information is accurate. Redistribute the updated list as needed.	Quarterly
Review the District's information systems and keep records identifying locations and systems that house personally identifiable information and other sensitive information: Ensure that confidential information is stored on a secure server that is accessible only with a password or other security protection. Keep and update records of all persons with access to District servers through personal or District-issued mobile devices and laptops and ensure that each device is password-protected and encrypted, as applicable. Ensure that District-maintained, cloud-based applications that use or maintain student or staff data, including criminal history record information, are compliant with the Family Educational Rights and Privacy Act (FERPA), the Children's Internet Protection Act (CIPA), CJIS Security Policy, and other federal and state law. Review requests from professional staff members for use of additional online educational resources, including review of the terms of service or user agreements, to ensure compliance with District standards and applicable law. Compile a list of third-party vendors with access to sensitive information, including the types of information and uses of the information. Issue a reminder to all relevant parties to secure sensitive paper records; password-protect records stored on thumb drives, external hard drives, and laptops; and dispose of records in accordance with the District's records retention requirements.	Quarterly

Review third-party vendor contracts: Coordinate with the business office to ensure that vendor contracts for cloud-based applications that use or maintain student or staff data are compliant with FERPA, CIPA, and other federal and state law. Ensure that contracts include breach notification.	At least annually
In coordination with the records retention officer, review data storage and disposal protocols to ensure that archived data meets industry standards and legal requirements for secure storage.	Annually
Update local security measures, including: System passwords, including a list of District employees with administrator access to information systems; Antivirus software (should update automatically); Firewalls; Data backup procedures; Data encryption procedures; and Data and records disposal best practices.	Quarterly
Monitor systems for data loss.	Continually
Conduct trainings with students, staff members, Board members, and others as needed on privacy and security awareness and District protocols for storing, accessing, retaining, and disposing of records.	Annually

Incident response team

Name	Position	Contact Information	Responsibility during Breach
Robert Bayard Jason Piazza Paul McLarty	Technology Coordinator/Chief Technology Officer Cybersecurity Coordinator/Director of Network & Technical Services Deputy Superintendent of Business and Support Services	281-284-0404 rbayard@ccisd.net 281-284-0435 jpiazza@ccisd.net 281-284-0180 pmclarty@ccisd.net	Notify the team. Identify the affected records.
Elaina Polsen	Chief Communications Officer	281-284-0022 epolsen@ccisd.net	Coordinate the notification and communications plan.
Leila Sarmecanic	General Counsel	281-284-0013 lsarmecanic@ccisd.net	Analyze the legal implications and advise the team regarding litigation risks and notification requirements.

Vendor list

The following outside vendors contract with the District for cloud-based (online) or other technology applications that have access to potentially sensitive student or staff information.

Name of vendor:	Vendor contact information:
Is vendor considered a “school official” for purposes of access to student records? (Circle one) Yes **No**	
Type of data:	Use of data/service provided:
Contract owner:	Date contract last reviewed for security compliance:

Name of vendor:	Vendor contact information:
Is vendor considered a “school official” for purposes of access to student records? (Circle one) **Yes** No	
Type of data:	Use of data/service provided:
Contract owner:	Date contract last reviewed for security compliance:

Name of vendor:	Vendor contact information:
Is vendor considered a “school official” for purposes of access to student records? (Circle one) Yes **No**	
Type of data:	Use of data/service provided:
Contract owner:	Date contract last reviewed for security compliance:

Responding to a potential breach

Note: For a breach involving criminal history record information, see DBAA.

Upon notification that a potential breach may have occurred, the Cybersecurity Coordinator or Technology Coordinator will immediately notify the incident response team and:

- ☐ Validate the facts that indicate a potential data breach;
- ☐ Determine the scope of the potential breach;
- ☐ Notify the District’s data breach coverage provider;
- ☐ Notify law enforcement, if needed;
- ☐ Determine whether there is a need for outside resources, such as privacy counsel, digital forensics examiners, credit monitoring services, and the like;
- ☐ Coordinate the incident response team and ensure that the team handles responsibilities in accordance with the nature and severity of the incident, including determining whether notification of affected individuals is appropriate and, if so, how best to provide the notification;
- ☐ Create, gather, and maintain all documents related to the incident; and
- ☐ Analyze information to determine the cause of the incident (internal cause, third-party breach, etc.) and take measures to address and remediate.