Data Breach Prevention and Response Plan

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

Cybersecurity Breach Prevention

Maintain and update the incident 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.	Semi-annually
Coordinate with the purchasing department to ensure that vendor contracts for software that use or maintain student or staff data are compliant with FERPA, CIPA, and other federal state law. Keep and update records of signed Data Privacy Agreements for all vendors that access student and staff data.	On Contract Renewal
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

UPDATED: 10/23/2023

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
Review cybersecurity training which is required to be completed annually by District employees and recommend any changes as needed.	Annually
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
Oversee and report findings of penetration tests, risk assessments, and/or vulnerability scans performed on the District.	Annually
Keep and update cybersecurity plans to combat cybersecurity incidents including but not limited to: Cybersecurity Plan Incident Response Plan Disaster Recovery Plan	Semi-annually

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;
- ☐ 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
- ☐ Follow the guidance of the internal Incident Response Plan.