McCall-Donnelly Joint School District #421

FACILITIES **Policy 9550**

Cybersecurity & Data Breach Response Policy

This policy aims to prevent data breaches and to ensure any such breaches are addressed quickly and appropriately. In pursuit of this, the Board directs the Superintendent or their designee to work toward implementing the National institute of Standards and Technology (NIST) Cybersecurity Framework.

Prevention Strategies

For the purposes of this policy, a data breach refers to any instance in which there is an unauthorized release or access of personally identifiable information or of other sensitive data. This can include, but is not limited to, student educational records, personnel records, and financial records. It can include situations such as malicious actors gaining access to District devices or systems; the loss of District devices; and devices or networks left unsecured by accident, negligence, or a security system failure.

Sensetive data shall mean data whose release could cause social, physical, or financial harm to the individual(s) it pertains to or to the District.

The Board emphasizes the following cybersecurity principles, which the Superintendent or designee shall draft procedures to implement:

1. Multifactor authentication for remote access and admin/privileged controls: To the extent feasible, phishing-resistant multifactor authentication will be required to access sensitive information and security-sensitive systems.

2. Endpoint detection and response: The Superintendent or their designee shall ensure all District devices are protected by endpoint protection including, but not limited to, antivirus software and any other appropriate measures to detect attempted breaches of network security. The superintendent or designee shall ensure District devices are safe when used at school and, if applicable, when used at other locations. They shall ensure steps are taken to block access to known malicious content online, to protect users from email-based attacks, and to ensure security updates are installed promptly.

3. Secured, encrypted, and tested backups: The superintendent or their designee shall ensure backups of important data are maintained securely to protect against data loss or destruction. They shall strive, when feasible, to ensure three backup copies of important data are kept, two of which are stored on different mediums, and one of which is stored at a separate physical site from the others. At least one of these copies should be stored on a device not connected to the internet.

4. Privileged access management: The superintendent or their designee will regularly

check that individuals who no longer need access to sensitive data and systems do not have access to them. This shall include ensuring access is immediately terminated when an individual's employment with the District is terminated or otherwise separated and when a student graduates or otherwise exits the District. To the extent feasible the Superintendent or designee shall ensure that duties are separated to prevent inappropriate access to or use of sensitive data. This also includes a requirement to ensure passwords are secure and are not shared. To limit risk, sensitive data will be safely archived or deleted when appropriate.

The superintendent or designee shall maintain an inventory of the District's physical and electronic assets related to cybersecurity that designated staff members should secure in the event of a possible disaster or data breach. These assets include, but are not limited to electronic files, logins, electronic devices, and equipment used to provide access to the internet and any District networks. The list shall indicate where these assets are stored and how they are protected.

The superintendent or designee shall also conduct privacy risk assessments for the District and of parties with whom it shares sensitive data. For this policy, privacy risk assessment shall mean a process to help analyze and assess privacy risks arising from the processing of their data.

Breach Response

The Superintendent or their designee shall check for signs of a data breach through such methods as automated tools, verifying whether current security measures are effective, searching online for signs of leaked data, and conducting tests of current security.

The Superintendent or designee shall create a Data Breach Response Plan for inclusion in the District's Crisis Management Plan. They may involve experts and stakeholders in the process of creating this plan. The Superintendent or designee may also conduct regular data breach drills or tests of portions of the Data Breach Response Plan. Those responsible for implementing the Data Breach Response Plan may be provided with training on or notification of the Plan regularly. The Superintendent or designee and any experts and stakeholders they choose to involve shall review the Plan annually to ensure it is current and that any appropriate improvements are made to it. Such review shall also take place following any suspected data breach.

The Superintendent or Designee shall direct staff to report any possible data breach to the Information Technology Director. Apart from such reporting, staff shall keep information about the breach confidential unless and until they have been assigned communication responsibilities related to the breach.

If the District identifies a lapse in security exposing sensitive information but is it unclear whether anyone has obtained or accessed such data, the District shall treat the incident as a data breach.

The District's Data Breach Response Plan shall include the following elements:

1. A process for determining whether a suspected breach is an actual breach and, if so, for learning about the nature of it, such as:
    a. Whether the breach is still active;
    b. The scope of the breach; and
    c. Whether the breach was accidental or malicious and whether it was internal or external.

2. The positions responsible for participating in the response to a possible data breach, including:
    a. An incident response leader and alternate leader who will coordinate such response;
    b. The Superintendent or their designated administration representative;
    c. Information technology staff;
    d. The District legal counsel;
    e. Communications or public relations personnel;
    f. Risk management personnel; and
    g. The business manager or designee.

    The plan shall also include the duties of each position, as determined by the Superintendent.

3. A process for deciding the appropriate course of action. This shall include:
    a. Choosing an individual or organization to investigate the breach;
    b. A listing of District resources available to address the breach and the authority who can approve their use;
    c. Fixing an active breach;
    d. Consulting with legal counsel to ensure legal requirements are met, including any federal, state, or district level requirements to notify outside authorities or victims of a breach;
    e. A plan for providing information about the breach if required or when communication is appropriate for the sake of transparency, to assist agencies working to prevent future breaches;
    f. Providing support to individuals who sensitive data was subject to the breach;
    g. Whether to report the incident to law enforcement and, if so, how to coordinate with them;
    h. Determining which outside organizations or individuals should be consulted or involved in the response, such as the Family Policy Compliance Office or other outside experts;
    i. Taking measures to preserve evidence of the breach and document the District's response;
    j. Determining the cause of the breach and how to prevent similar breaches in the future, such as through technological fixes, training, or other measures; and
    k. A plan for maintaining continuity of District operations through the breach. This plan shall include details on the keeping and use of data backups.

Thid Parties

The Superintendent or their designee shall take measures to limit risk when using third party tools or services and when it is necessary to share sensitive data with third parties.

They shall also regularly review such third parties' policies on data breach notifications and backing up data or ensure these topics are addressed adequately in the District's contract with such providers.

Legal Compliance and Insurance

The Superintendent or their designee shall report any cybersecurity incident to the Office of the Attorney General within 24 hours as required by IC 28-51-105. When required, the incident shall also be reported to the Idaho Superintendent of Public Instruction and the Executive Director of the Office of the State Board of Education.

The Superintendent or designee shall record any breach of education records in the log of releases of information described in Policy 3620 – Student Records. Any cybersecurity incident shall also be reported to the federal Cybersecurity and Infrastructure Security Agency if required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 or, in cases where reporting is optional if the Superintendent chooses to do so.

In the event of any cybersecurity event, the Superintendent or designee shall immediately contact their cybersecurity insurance provider and, if applicable, the District's managed security provider.

Legal Reference:

32 CFR 99.32(a)(1)	What Recordkeeping Requirements Exist Concerning Requests and Disclosures?
CIRCIA	Cyber Incident Reporting for Critical infrastructure Act of 2022
IC 28-51-104	Definitions
IC 28-51-105	Disclosure of Breach of Security of Computerized Personal Information by an Agency, Individual or Commerical Entity

Policy History:

Adopted: