

Billings School District 2

NONINSTRUCTIONAL OPERATIONS

Data Breach Policy

Purpose

This policy is established to ensure Billings Public Schools (the "School District") follows a routine response regarding the notification of data breaches that involve personal information. The District is committed to safeguarding personal information of students, staff, and community members and to responding promptly and appropriately in the event of a data breach.

Scope

This policy applies to all employees, contractors, and third-party service providers of Billings Public Schools who have access to computerized data containing personal information.

Definitions

“Data Breach” or “Unauthorized acquisition of computerized data”: means the unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the School District or by a third party on behalf of the School District, and causes or is reasonably believed to cause loss or injury to a person.

“Personal Information”: means an individual's first name or first initial and last name combined with any one or more of the following data elements when the name and data elements are not encrypted: social security number, driver's license or state issued identification number, a tribal identification number or enrollment number, or similar identification issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Commonwealth of Northern Mariana Islands, the Virgin Islands, or American Samoa, an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account, medical record information as defined in Mont. Code Ann. §33-19-104, taxpayer identification number, or identity protection numbers issued by the IRS. This definition specifically excludes publicly available information from federal, state, local, or tribal government records.

Responsibilities and Procedures

a. Discovery of a Breach

Employees must immediately report any suspected or confirmed data breach to the School District's Director of Technology, or an employee otherwise designated as the Data Breach Coordinator.

b. Investigation

Upon notification of a potential Data Breach, the Director of Technology or Data Breach Coordinator will initiate an internal investigation to determine the scope and impact of the Data Breach in collaboration with IT staff. If a Data Breach is confirmed, law enforcement will be contacted by the Director of Technology or the designated Data Breach Coordinator.

c. Notification Requirements

If it is confirmed that a Data Breach concerning Personal Information has occurred by an unauthorized person, the School District shall make reasonable efforts to notify the affected individuals without unreasonable delay, consistent with the legitimate needs of law enforcement or with any measures necessary to determine the scope of the Data Breach and to restore reasonable integrity of the data system.

Notification must be provided through at least one of the following methods: Written notice provided via email or mailed to the last known address of the individual in question, Electronic notice, consistent with applicable electronic record laws, or telephonic notice.

d. Third-Party Notifications:

If a Data Breach is experienced by a third party holding personal information on behalf of the School District, the third party must promptly notify the School District. The School District will not have an independent duty to notify in the situation of a third-party data breach unless the third party requests to partner with the School District for proper notification.

e. Compliance with Law Enforcement:

Notification may be delayed if law enforcement advises that it could impede an investigation. The District will comply with such requests and notify impacted individuals as soon as permissible.

f. Reporting to Authorities

The School District will simultaneously submit an electronic copy of the notification to the chief information security officer at the Department of Administration and to the Attorney General's consumer protection office, excluding personal identifying information, and will include a statement that details the date and method of notification. Such notification will specify the number of people receiving notification of the Data Breach.

//

//

g. Security Measures

Billings Public Schools will maintain an information security policy designed to safeguard personal information and regularly train staff on security protocols and breach response procedures.

Enforcement

Compliance with this policy is mandatory, and any employee who fails to adhere to this policy by not immediately reporting and/or responding as described in the policy may be subject to disciplinary action, up to and including termination.

Policy History:

First Reading: November 17, 2025

Second Reading: December 2, 2025

Third Reading: December 15, 2025

Adopted on: December 15, 2025

Revised on: