Data Privacy Breach Policy and Procedure

Document Information

Last revision date:	April 16, 2018	
Adopted date:		
Next review:	January 1 Annually	

Overview

A privacy breach is an action that results in an inappropriate use of the Personally Identifiable Information (PII) of students or the disclosure of this information to the wrong recipient. The Sherburne-Earlville CSD's highest priority is to respond to any privacy breach with immediate measures to limit damaging effects.

Examples of a privacy breach may include:

- An employee or contractor intentionally or unintentionally transmits or discloses records containing student PII to an unauthorized party.
- A device with student data, or with access to student information, is lost or stolen.
- A system that contains student records or data is accessed by an unauthorized user.
- Student data, either in hard copy form, on a device or on a system is not properly disposed of.
- Student information is disclosed on a telephone call to people who are not authorized to hear the information.
- Student names or information are transmitted on social media.

Breach Reporting and Response

All Sherburne-Earlville CSD employees have a role in safeguarding student information and responsibility for immediately communicating and containing damage in the event of a privacy breach. Employees who become aware of a suspected or actual security breach must report the matter immediately to their Principal or Supervisor. If their Principal or Supervisor is not available, the incident must be reported to an alternate Principal, Supervisor, or the District Office.

Step 1: Initial Information Gathering

After a suspected or actual privacy breach is reported, the Principal or Supervisor will implement the following actions:

1. Contact the Superintendent of Schools or designee.

2. Record the date and time when the suspected or actual breach was discovered and the date and time when response efforts began.

3. Identify all internal and external resources who can contribute knowledge to confirm whether or not a breach has actually occurred or the extent of the breach.

4. Suspend the process that is causing the privacy breach if further breaches occur.

Step 2: Assemble District Breach Response Team

Responsibilities must be assigned so that the remaining steps may be followed in a timely and orderly manner. The response team will consist of the following individuals:

1. The Superintendent of Schools or designee.

2. The Principal and departments whose teams must respond to the breach and staff who must be directly involved in containment efforts.

3. BOCES and/or South Central Regional Information Center staff to support district teams.

Clearly articulate among team members what can and cannot be communicated at this point and to whom with the purpose of preventing further privacy risks or conjecture among the public that could lead to an inaccurate representation of what happened.

Step 3: Secure and Contain

The Breach Response Team must first contain the breach to ensure that no further damage is done. The team will first focus on the following actions:

1. Secure the premises around the area where the breach occurred to help preserve evidence (if applicable).

2. Stop additional data loss by taking machines or systems off-line, disconnecting network access, changing passwords, blocking access through firewalls, etc.

Efforts must be made to not turn-off or reboot systems in a way that will create a loss of logs or information that will be useful forensic information for uncovering the root cause of the breach.

Step 4: Document Everything

Everything that is known about the breach must be documented (see the checklist at the end of this document).

1. The documentation should address the standard who, what, where, why and how questions and also what is not known. Including who discovered the breach, who reported it, to whom it was reported, who else knows about it, what type of breach occurred, what information was disclosed, what was stolen/is missing, how it was stolen, what systems are affected, etc.

2. Interviews with persons involved in discovering the breach and anyone else who knows about it must be conducted and documented.

Step 5: Contact Authorities

As directed by the Superintendent of Schools or designee, legal counsel should be contacted to advise the district on the matter, and, in the case of theft of equipment, a break-in or other criminal activity, police should be contacted as appropriate.

Step 6: Investigate

A full investigation of the privacy breach must be conducted and a written report prepared addressing the following aspects of the incident:

1. Identification and analysis of the events that led to the breach with supporting documentation and interview statements.
2. Identification and assessment of actual and potential risks.
3. A summary of relevant policy and procedures that have bearing on the incident.
4. A review of what was done to contain the breach.
5. Recommendations for remedial action so future breaches do not occur.

Step 7: Notify

Notification must be sent to the effected individuals whose privacy has been compromised along with a description of the information that was compromised. The notice of privacy breach will include:

- A description of what happened.
- The actual and/or potential risks.
- The mitigating actions taken by the district.
- What actions the effected individuals should take to protect themselves against harm.

Step 8: Improvement and Remediation

It is essential that the district continually improve safeguards to prevent future privacy breaches from happening. To these ends, the district will implement the remedial actions that are identified and take any other actions that may strengthen privacy and security including:

- Reviewing the relevant processes to enhance compliance with privacy legislation.
- Amending or reinforcing existing policies, procedures and practices for managing and safeguarding student PII.
- Developing and implementing new security or privacy measures.
- Implementing additional staff training to promote awareness and focus frontline security efforts.

Employees who have been found to be in violation of security and privacy policies may be subject to remedial action, disciplinary measures or termination of employment based on the nature and severity of the offense. Such measures will be implemented in accordance with district policies and procedures and relevant union contracts.

Privacy Breach Investigation Checklist

- ✓ Provide a detailed account of what happened.
- ✓ How did the breach occur?
- ✓ What type of student data is involved? Identify individual data fields (i.e. name, address, student grades, locker number, etc.).
- ✓ How many students or records are involved?
- ✓ What happened to the data?
- ✓ Establish a detailed timeline indicating when the breach occurred, when it was detected, who detected the breach, when was the breach was contained, etc.
- ✓ What actions did the district take to mitigate the breach?
- ✓ Were there any protections in place? (i.e. encryption, passwords, locked doors, etc.).
- ✓ What are the potential adverse consequences for students or the district?
- ✓ How serious or substantial are they and how likely are they to occur?
- ✓ What could the data tell a third party about an individual?
- ✓ What harm could this cause?
- ✓ What commercial value does the information have?
- ✓ What processes/systems are affected and how?
- ✓ What steps can be taken to prevent this from happening in the future?
- ✓ What additional training is needed to prevent this from happening again?