

LEA Model: Data Breach

The guidance and checklist in this document is provided by USBE for Utah LEAs as general examples illustrating some current industry best practices in data breach response and mitigation applicable to the Utah education community. USBE is providing these documents to support LEAs in their implementation of requirements under §53A-1-1405, however LEAs should develop policies that reflect their individual needs and priorities, and seek legal counsel to ensure that the policies follow federal and state law, and board rule.

A data breach is any instance in which there is an unauthorized release or access of PII or other information not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider. Data breaches can take many forms including:

- hackers gaining access to data through a malicious attack;
- lost, stolen, or temporarily misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.);
- employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff mis-configuring a security service or device, etc.); and
- policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable)

To prevent a data breach, LEAs should prepare and maintain data privacy and security policies and procedures in accordance with industry best practices, and as required under Utah state law. Some key components to a strong policy might include:

- Implement appropriate technical, administrative and physical security safeguards
- Review your information system(s) and data and identify where PII and other sensitive information resides
- Continuously monitor for PII and other sensitive data leakage and loss
- Consider establishing relationships with outside advisors who are knowledgeable about data breaches (e.g., IT, forensics and counsel)
- Track data breach laws, rules and notification mandates
- Prepare and implement a data breach response policy and procedure (see suggested checklist)
 - Assemble a data incident response team and applicable roles
 - Outline critical steps to take within the first 24 hours of a suspected breach
 - Train staff to identify and report suspected breaches
 - Conduct a practice data breach response scenario

If a breach occurs, LEAs should have a protocol in place for response. Utah law §53A-1-1405 further requires LEAs to notify adult students or parents/legal guardians in the event of a breach involving student data. The check-list provided in this guidance was adapted from guidance provided by the US Department of Education's Privacy Technical Assistance Center (ptac.ed.gov) and can be used as a model for how to respond to a breach.

Additional Resources for LEAs:

[PTAC Guidance and checklist](#)

[Data Breach Response Training Kit](#)

Sample Policies

[LEA Policy Template, Provided by Colorado Department of Education](#)

[University of Vermont](#)

[Kentucky Department of Education](#)

Sample Notifications

[Online notification](#)

[Good example of continued updates and communication of progress](#)

[Lost/misplaced thumb drive](#)

[Inadvertent disclosure of PII to media](#)

[Phishing attempt with possible compromise of staff PII](#)

[Office break-in and theft of computer with files containing staff PII](#)

[Student records database accessed with grade changes](#)

Data Breach Response Best Practices Checklist

- Validate the data breach
 - a. Confirm breach has ended and lock-down of systems (e.g., change passwords and encryption keys)
 - b. Isolate and preserve compromised systems and data
- Assign an incident manager to be responsible for the investigation
- Assemble your Data Breach Response Team
 - a. Suggested stakeholders, as appropriate: School and District leadership, Legal, IT Security, Information Technology, your appointed Student Data Manager, Human Resources, Internal Auditors, District Communications/Public Relations
- Investigate scope of breach to determine types of information compromised and number of affected individuals
- Decide how to investigate the data breach to ensure that the investigative evidence is appropriately handled and preserved
- Attempt to retrieve lost or otherwise compromised data
- Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification
 - a. Identify notification timeframes and requirements
 - b. Develop and deliver notices to affected individuals and agencies in accordance with regulatory mandates and timeframes
- Determine whether to notify the authorities/law enforcement (situation dependent)
 - a. Involve counsel to analyze legal obligations

Tips:

- Document your work, but coordinate with counsel on preparation and treatment of written materials related to the breach
- Act swiftly, as regulatory timeframes begin upon discovery of the breach
- Evaluate the need for a toll-free number for affected individuals to receive specific information and assistance
- Consider offering credit monitoring, identity repair services, or identity theft insurance for affected individuals
- Cooperate with regulatory and governmental inquiries

Sample Data Breach Letter Best Practices

DISTRICT LETTERHEAD

[PARENT OR LEGAL GUARDIAN NAME]

[STREET ADDRESS]

[CITY, STATE AND ZIP CODE]

[DATE]

Dear [PARENT OR LEGAL GUARDIAN NAME],

The first paragraph should reaffirm your school and district's commitment to data privacy. It should say that there has been a breach and that you are committed to protecting students, staff and their privacy.

What Happened?

Next, you should include a brief description of the data breach incident in general, and accessible terms. Avoid too much jargon or technical information that might leave you vulnerable again. Details should include the date of the breach or, if unknown, the approximate date or date range of the breach. You could describe whether data was hacked, mistakenly sent insecurely, if a computer or other device was forgotten or lost, or if there was a physical break-in or theft.

What information was involved?

Recipients will want to know what data was breached. If you know the data that was compromised, provide as much detail as possible without further compromising your security systems (see example letters for ideas).

What is [LEA NAME] doing in response?

Provide a brief description of the actions taken by the school or district to contain the breach and protect data from further unauthorized access or use. For example, did you require every user to change their password? Did you restore your gradebooks to the state they were prior to the breach? Did you verify the recipient deleted all copies of the inadvertent data sent to them?

If this notice was delayed because of law enforcement investigation, you should explain that so you can be clear about the timeline of your response.

What is [LEA NAME] doing to prevent this from happening in the future?

Here, recipients will want to know what steps you have implemented, or will implement, to prevent this type of breach. Of course, there is no way to anticipate all possible threats, but you can use this as an opportunity to reexamine your policies, procedures, training, and audit/review regarding data privacy. Analyze the root cause of the situation and identify where your vulnerabilities are.

What additional steps you can take?

Next, provide information on resources available to and advice on actions affected individuals should take. If the breach involves social security numbers or other potentially vulnerable PII, you should consider providing free credit monitoring for affected parties for 1 to 2 years and provide information on how to sign up for the service. If student educational records were compromised, remind parents or

legal guardians how to review the educational record and their rights to correct any errors.

Where can you get more information on this issue?

Here, list all relevant contact information for the individual at the district who can answer questions, law enforcement or other government authorities and, as appropriate, contact information for national consumer reporting agencies.

Close by once again reaffirming your LEA's commitment to privacy and a great education.

Sincerely,

X _____

[LEA Name] [Superintendent or other relevant leader]