

Sherman Central School Data Breach Policy

INCIDENT REPORTING AND NOTIFICATION

- Educational agencies shall report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer and notify impacted stakeholders. To learn more about this requirement, agencies can review Part 121.10 of the Regulations.

REQUIREMENTS FOR THIRD PARTY VENDORS

1. Notification of Data Breach

- a. Vendor shall promptly notify the District of any Data Breach in the most expedient way possible and without unreasonable delay, but no more than seven calendar days after Vendor discovers or has been informed of such breach.
- b. Vendor shall provide such notification to the District by contacting the District's Data Protection Officer, Mr. Mike Shimmel (the "District's DPO"), directly by email at mshimmel@shermancsd.org or by calling 716-761-4805.
- c. Vendor shall cooperate with the District and provide as much information as possible directly to the District's DPO or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- d. Vendor acknowledges that upon initial notification from Vendor, the District is obligated under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department (the "CPO"). Vendor shall not provide such notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor shall promptly inform the District's DPO or his/her designee, but no later than two calendar days of having received such request.

REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES

- REPORTING REQUIREMENTS
 - 10 DAYS TO REPORT TO NYSED

- The agency must report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer no more than 10 calendar days after such discovery.
- NOTIFICATION REQUIREMENTS
 - 60 DAYS TO NOTIFY AFFECTED INDIVIDUALS
 - The agency must notify affected parents, eligible students, teachers and/ or principals no more than 60 calendar days after the discovery of a breach or unauthorized release.
- LAW ENFORCEMENT OR VULNERABILITY DELAY
 - Where notification is delayed, the agency must notify affected individuals within 7 calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.
- THIRD-PARTY REIMBURSEMENT REQUIREMENT
 - Where a breach or unauthorized release is attributed to a third-party contractor, the contractor must pay for or reimburse the agency for the full cost of notification.
- METHOD OF NOTIFICATION
 - Notification must be directly provided to the affected individuals by first- class mail to their last known address; by email; or by telephone.
- CONTENTS OF NOTIFICATION
 - Notifications must be clear, concise, use language that is plain and easy to understand, and to the extent available, include:
 - a brief description of the unauthorized release
 - the dates of the incident and date of discovery
 - a description of the types of PII affected
 - the number of records affected
 - a brief description of the agency's investigation
 - contact information for representatives who can assist parents