

SpEd Forms, LLC

Data Privacy Policy

Purpose and Scope

The purpose of this policy is to describe the duties and responsibilities to protect student data transmitted to SpEd Forms from customers pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, HIPAA and applicable local State law. In performing these services, the SpEd Forms shall be considered a School District Official with a legitimate educational interest, and performing services otherwise provided by the customer. With respect to the use and maintenance of Student Data, SpEd Forms shall be under the direct control and supervision of the customer.

SpEd Forms may receive or create, and the customer may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA"), Children's Online Privacy Protection Act ("COPPA"), Protection of Pupil Rights Amendment ("PPRA"). Protected Health Information (PHI) is covered under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

The documents and data transferred from customers and created by the our services are also subject to the customer's State student and health care privacy laws.

Data Ownership

Data Ownership: All Student Data transmitted to the SpEd Forms pursuant to the Service Agreement is and will continue to be the property of and under the control of the customer. SpEd Forms further acknowledges and agrees that all copies of such Student Data transmitted to us, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this policy in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the customer. For the purposes of FERPA and HIPAA, the SpEd Forms shall be considered a School District Official, under the control and direction of the customer as it pertains to the use of Student Data notwithstanding the above.

Parent Access: The customer shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. SpEd Forms shall respond in a timely manner (and no later than 30 days from the date of the request) to the customer's request for Student Data in a pupil's records held by the SpEd Forms to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the SpEd Forms to review any of the Student Data

accessed pursuant to the Services, SpEd Forms shall refer the parent or individual to the customer, who will follow the necessary and proper procedures regarding the requested information.

Third Party Request: Should a Third Party, including law enforcement and government entities, contact SpEd Forms with a request for data held by us pursuant to the Services, SpEd Forms shall redirect the Third Party to request the data directly from the customer. SpEd Forms shall notify the customer as soon as possible in advance of a compelled disclosure to a Third Party.

Subprocessors: SpEd Forms shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this policy, as well as state and federal law.

Duties of the customer

1. **Privacy Compliance.** customer shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, HIPAA and applicable State law.

2. **Annual Notification of Rights.** The customer shall include a specification of criteria under FERPA for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. **Reasonable Precautions.** customer shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification.** customer shall notify SpEd Forms promptly of any known or suspected unauthorized access. customer will assist SpEd Forms in any efforts by SpEd Forms to investigate and respond to any unauthorized access.

Duties of SpEd Forms

1. **Privacy Compliance.** The SpEd Forms shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, HIPAA and applicable State law.

2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes. SpEd Forms also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the customer.

3. **Employee Obligation.** SpEd Forms shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this policy with respect to the data shared under the Service Agreement.
4. **No Disclosure.** SpEd Forms shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.
5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, SpEd Forms shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any student data; (2) erasing; or (3) otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes SpEd Forms to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. SpEd Forms shall provide written notification to the customer when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified pursuant to the other terms of this policy. The customer may request a Student Data restore by submitting a support request or calling our support line. Upon receipt of a request from the customer, the SpEd Forms will immediately provide the customer with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.
 - a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, the customer may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed.
 - b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement SpEd Forms shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data. In no event shall SpEd Forms dispose of data pursuant to this provision unless and until SpEd Forms has received affirmative written confirmation from customer that data will not be transferred to a separate account.
6. **Advertising Prohibition.** SpEd Forms is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a SpEd Forms; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to customer; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to customer. This section does not prohibit SpEd Forms from using Student Data for adaptive learning or customized student learning purposes.

DATA PROVISIONS

1. Data Security.

The SpEd Forms agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of SpEd Forms are set forth below. These measures shall include, but are not limited to:

- a. **Passwords and Employee Access.** SpEd Forms shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. SpEd Forms shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
- b. **Destruction of Data.** SpEd Forms shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to customer or customer's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes SpEd Forms to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. SpEd Forms shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by customer.
- d. **Employee Training.** The SpEd Forms shall provide periodic security training to those of its employees who operate or have access to the system. Further, SpEd Forms shall provide the customer with contact information of an employee who customer may contact if there are any security concerns or questions.
- e. **Security Technology.** When the service is accessed using a supported web browser, SpEd Forms shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. SpEd Forms shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. **Security Officer.** SpEd Forms' security officer is Mark Oehrlein.

g. **Subprocessors Bound.** SpEd Forms shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this policy. SpEd Forms shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this policy.

h. **Periodic Risk Assessment.** SpEd Forms further acknowledges and agrees to conduct digital and physical periodic (no less than annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

Data Breach

In the event that Student Data is accessed or obtained by an unauthorized individual, SpEd Forms shall provide notification to the customer within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. SpEd Forms shall follow the following process:

- a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
- b. The security breach notification described above in section a shall include, at a minimum, the following information:
 - i. The name and contact information of the reporting customer subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed because of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c. At customer's discretion, the security breach notification may also include any of the following:

- i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. SpEd Forms agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- e. SpEd Forms further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide customer, upon request, with a copy of said written incident response plan.
- f. SpEd Forms is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by the customer. If customer requests SpEd Forms's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to SpEd Forms, SpEd Forms shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.
- g. In the event of a breach originating from the customer's use of the Service, SpEd Forms shall cooperate with customer to the extent necessary to expeditiously secure Student Data.