Student Data Privacy Special Terms and Conditions

Contents

Parties

This Student Data Privacy Special Terms and Conditions (hereinafter "Agreement") is by and between _____ ("District"), a public school district located in the City/Town of _____in the State of Rhode Island and _____("Vendor"), a contractor performing institutional services and functions that will require student data to perform those services and functions, whose principal place of business is located in _____.

Purpose/Description of Service

Vendor acknowledges and agrees that this Agreement is for any services which requires the use of student data. These services are for the purpose of sharing Data Files (defined below) between the parties in a manner consistent with the Family Education Records Privacy Act of 1974 ("FERPA")") and Rhode Island's Identity Theft Protection Act of 2015, RI General Laws Section 11-49.3 ("State Regulations").

The Data Files shall be used by the Vendor and its employees to populate student data only for the purpose of delivering the Services agreed upon. Vendor further acknowledges and agrees that all copies of such Data Files, including any modifications or additions to Data Files or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Data Files.

Definition, Use and Treatment of Data

In the course of performing Services, the Vendor will obtain confidential student data. Student data includes all Personally Identifiable Information ("PII") Personal health information ("PHI"), directory data, confidential student record information, and other non-public information. This data includes, but is not limited to student data, metadata (e.g. logs, cookies, web beacons, etc.), and user content ("Data Files"). Any data or metadata a 3rd party will collect (e.g. analytics, etc.) is a function of the use of the provider's service.

The term "Vendor" shall include the contractor performing services for the District, its employees, agents, assigns, subcontractors, other third parties working in conjunction with or on behalf of the contractor.

No Marketing or Advertising

The vendor is prohibited from using Confidential Data to (a) market or advertise to students or families / guardians; (b) inform, influence or enable marketing, advertising or other commercial

efforts by a third party; or (c) develop a profile of a student, family member / guardian or group, for any commercial purpose other than providing the Service to District.

Data De-Identification

Vendor may not use any Data including de-identified data for product development, or research without specific written approval obtained prior to the use thereof. In such case, Vendor shall remove all direct and indirect personal identifiers, including any data that could be analyzed and linked to other data to identify the student or family member / guardian. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location data, and school ID.

Vendor shall not attempt to re-identify de-identified Confidential Data and not to transfer de-identified Confidential Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) Vendor gives prior notice to District and District provides prior written consent. Vendor may use de-identified Confidential Data for internal product development and improvement, and research.

Notification of Amendments to Policies

A. Vendor shall not change how Confidential Data are collected, used or shared under the terms of the Agreement, without advance notice to and prior written consent from District.
B. Vendor shall provide prior notice to District of any proposed change to its terms of service, terms and conditions of use, license agreement and/or privacy policies, at least thirty (30) days prior to the implementation of any such change.
C. Such proposed changes may only be instituted with written approval from the District.

Data Transfer upon Termination or Expiration

A. Upon termination or expiration of the Agreement, Vendor will ensure that all District Data are securely returned or destroyed as directed by the District. Transfer to the District or a third party designated by the District shall occur within a reasonable period of time, and without significant interruption in service. Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition.
B. Vendor will notify the District of impending cessation of its business and any contingency plans. Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the District. Vendor will work closely with its successor to ensure a successful transition.

Data Collection

Vendor shall only collect, process and store the Confidential Data that are necessary to provide the Service to District under this Agreement. Vendor shall not collect, process or store Confidential Data or other data related to students, families or guardians that are available from third parties.

Data Analysis and Mining

Vendor is prohibited from analyzing or mining Confidential Data for any purpose other than delivering the Service to District under this Agreement, or improving the Service for District. Analysis and mining of Confidential Data to support marketing, advertising or other commercial ventures, whether by Vendor or a third party, are prohibited.

Data Sharing and Re-Disclosure

Vendor is prohibited from sharing data without prior written consent of the District except as required by law.

Vendor will ensure that all sub-contractors are aware of this agreement and that each sub-contractor agrees to be bound by the terms and conditions.

District understands that Vendor may rely on one or more sub-contractors to provide the Service under this agreement, who may have access to Confidential Data. Vendor shall provide District with the name, address and other information as reasonably required by the District regarding each such sub-contractor prior to sharing any data.

Through the term of the agreement, Vendor shall also provide prior notice to District if Vendor plans to engage a sub-contractor who may have access to Confidential Data.

In each instance, the District may prohibit data sharing with any sub-contractor, if District does not approve of the sub-contractor. Such approval shall not be unreasonably withheld. However, at a minimum, Vendor must provide reasonable assurances that the subcontractor shall be bound to the same terms and conditions in this agreement.

Vendor is prohibited from further disclosing any Confidential Data unless re-disclosure is:

A. only in furtherance of providing the Service to District, and recipients of re-disclosed Confidential Data agree in writing to comply with these Student Data Privacy Special Terms and Conditions and related federal and state laws / regulations that protect Confidential Data, or;
B. required to ensure legal and regulatory compliance, or;
C. in response to a judicial process in a court in the USA, or;

D. to protect the privacy of Confidential Data, the safety of users or others, or the security of the Service.

If any of the four permitted re-disclosure events noted above occurs, Vendor shall immediately notify District.

Data Transfer and Destruction

Vendor acknowledges and agrees, upon notice from District, to ensure that:

A. A complete, readable and usable copy of all Confidential Data in Vendor's possession will be delivered to District within 60 days following notice from District; and
B. This copy of all Confidential Data will be provided in a standard format with standard delimiters and a matching data dictionary, mutually agreeable and sufficient to enable efficient transfer of the Confidential Data to a new system; and
C. This copy must include all Confidential Data which may have been re-disclosed to or held by sub-contractors or agents of Vendor; and
D. Following notice of acceptance of this copy of all Confidential Data by District, Vendor will permanently destroy all copies of Confidential Data held by Vendor or re-disclosed by Vendor, e.g. to Vendor's agents, sub-contractors or business partners. Permanent destruction of this Confidential Data must be non-recoverable and meet DoD standard 5220.22-M[1] and processes recommended by NIST Special Publication 800-88[2]; and
E. Within 90 days of notice, Vendor will deliver a written confirmation to District certifying that the permanent destruction of all Confidential Data held by Vendor and Vendor's sub-contractors, agents and business partners has been completed.

Rights and License to Confidential Data and Intellectual Property

The Vendor acknowledges and agrees that:

A. All rights to Confidential Data and derivative works created from Confidential Data shall remain the exclusive property of District; and
B. All rights to District Intellectual Property (IP) shall remain the exclusive property of District and District students and staff; and
C. Vendor may not sell, trade, rent, lease or otherwise profit from the transfer of Confidential Data or District IP; and
D. District grants to Vendor a limited, nonexclusive license to use, process and store the Confidential Data and District IP solely for the purpose of delivering the Service to District under the terms of the Agreement; and

[1] Department Of Defense (DoD) Media Sanitization Guidelines 5220.22M
[2] NIST Special Publication 800-88, Guidelines for Media Sanitization

E. This limited, nonexclusive license granted to Vendor by District expires when the Agreement is terminated.

Confidential Data: Access, Changes, Copies and Removal

Vendor acknowledges and agrees, that upon District's request, any Confidential Data held by Vendor will immediately be made available to District, may be changed by District, may be deleted in whole or in part by District, and may be copied by District.

Security Framework and Standards

Vendor certifies that it will operate the service and collect, process and store Confidential Data in accordance with NIST data security standards and current industry best practices, and maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of Confidential Data, and prevent unauthorized access, disclosure and use. Vendor shall:

A. Restrict access to the Service and Confidential Data to only those individuals that require access in order for Vendor to provide the Service to District; and
B. Establish user IDs and authentication as necessary to protect access to Confidential Data, and protect all such user credentials from unauthorized access or use; and
C. Always protect all Confidential Data with strong encryption, at rest and in transit; and
D. Prevent hostile or unauthorized intrusion that could compromise confidentiality, result in data corruption, or deny access to or the proper operation of the Service; and
E. Prevent and detect computer viruses and malware from spreading through the use of the Service, e.g. via e-mail, files, documents, messages, other data or the required use of insecure District-side applications; and
F. Detect and prevent the unauthorized re-disclosure of Confidential Data by Vendor employees or agents; and
G. Provide prior notice to District of any planned system change that may impact the security of Confidential Data; and
H. Retain an experienced data security company, at least once per year, to thoroughly audit Vendor's IT infrastructure, systems, applications and processes to uncover vulnerabilities, and make prompt and reasonable efforts to remediate all vulnerabilities discovered; and
I. Provide District with a complete copy of Vendor's then-current security audit report, including details on all vulnerabilities discovered, and;
J. Immediately notify District if any incident occurs that might impact the reliable provision of the Service or security of Confidential Data, e.g. the discovery of unauthorized access, a malicious attack on the Service or Confidential Data, loss of a device containing Confidential Data, or the presence of malware. Such notice shall be made within no more than 10 days after discovery of such incident or condition.

Data Breach

Vendor acknowledges and agrees to notify the District's designated representative in writing within three (3) days of its determination that it has experienced a data breach, breach of security, privacy incident or unauthorized acquisition or use of any Data Files and/or any portion thereof contained therein.

The Vendor shall promptly investigate the Data Breach and provide District with detailed information about the Data Breach, including the identity of affected individuals.

The Vendor certifies it will fully comply with 11-49.3-1, et seq as amended from time to time and all other applicable state laws. In accordance with Rhode Island's Identity Theft Protection Act of 2015 § 11-49.3-4 "Notification of breach", the Vendor will send notifications to all affected parents, legal guardian, or eligible students. The notifications shall be made in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach.

Vendor agrees that said notification shall include, to the extent known:

A. A general and brief description of the incident, including how the security breach occurred and the number of affected individuals;
B. The type of information that was subject to the breach;
C. Date of breach, estimated date of breach, or the date range within which the breach occurred;
D. Date that the breach was discovered;
E. A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact:
    a. The credit reporting agencies
    b. Remediation service providers
    c. The attorney general;
F. A clear and concise description of the affected parent, legal guardian, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

In the event of a reportable breach, the Vendor shall keep a complete copy of the District's data it held at the time of the breach in a District approved secured, encrypted form and format. Vendor shall retain said data on the District's behalf unless and until the District directs its transmission or certified destruction.

If the District chooses to investigate such breach, the Vendor shall provide its full and complete cooperation without cost or charge to the District.

Cyber Liability Insurance

The Vendor shall obtain cyber liability insurance. The Vendor's cyber policy shall include:

A. Coverage for both, first- and third-party insurance, for cyber losses.
B. First-party coverage insures for losses to the policyholder's own data or lost income or for other harm to the policyholder's business resulting from a data breach or cyber-attack.
C. The District shall be covered as a first party insured.
D. Third-party coverage insures for the liability of the policyholder to third parties — including Districts and governmental entities — arising from a data breach or cyber-attack.
E. Said policy shall include provisions for remediation including: a call center or similar capacity to promptly field complaints and questions; one year of creditor monitoring and one year of credit insurance in minimum amount of one million dollars per incident.
F. The insurance policy shall include a thirty day notice of cancelation provision which includes notice to the District.

District shall be provided a copy of the insurance policy or other evidence of coverage, as requested by the District from time to time.

Litigation Hold

Vendor acknowledges and agrees, upon receipt of a litigation hold request from District, to immediately implement a litigation hold and preserve all documents and data relevant identified by District and suspend deletion, overwriting, or any other possible destruction of documentation and data identified in, related to, arising out of and/or relevant to the litigation hold.