Vendor Name: B.E. Publishing

APPENDIX - Data Security and Privacy Agreement for FY 2017/18 (July 1, 2017-June 30, 2018)

ARTICLE 1 – PROTECTED INFORMATION

Vendor acknowledges that its performance of Services under this Agreement may involve access to confidential District information including, but not limited to, personally-identifiable information, student records, protected health information, or individual financial information (collectively, "Protected Information") that is subject to state or federal laws restricting the use and disclosure of such information, including, but not limited to, Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civil Code § 1798 et seq.); the California Confidentiality of Medical Information Act (Civil Code § 56 et seq.); the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164). Vendor agrees to comply with all applicable federal and state laws restricting the access, use and disclosure of Protected Information. Vendor agrees to include all of the terms and conditions contained in this Appendix in all subcontractor or agency contracts providing services under this Agreement.

All Protected Information is wholly owned by, and shall be under the control of the District.

ARTICLE 2 – COMPLIANCE WITH FAIR INFORMATION PRACTICE PRINCIPLES

With respect to the District's Protected Information, and in compliance with all applicable laws and regulations, Vendor shall comply in all respects reasonably pertinent to the Agreement with the Fair Information Practice Principles, as defined by the U.S. Federal Trade Commission.

ARTICLE 3 – PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED INFORMATION

Contractor agrees to hold the District's Protected Information, and any information derived from such information, in strictest confidence. Vendor shall not access, use or disclose Protected Information except as permitted or required by the Agreement or as otherwise authorized in writing by District, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected Information, Vendor will notify District in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give District an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Any transmission, transportation or storage of Protected Information outside the United States is prohibited except on prior written authorization by the District. Vendor and its agents or third parties is prohibited from using any personally identifiable information in pupil records to engage in targeted advertising.

ARTICLE 4 – SAFEGUARD STANDARD

Contractor agrees to protect the privacy and security of Protected Information according to all applicable laws and regulations, by commercially-acceptable standards, and no less rigorously than it protects its own confidential information, but in no case less than reasonable care. Vendor shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of the Protected Information. All Protected Information stored on portable devices or media must be encrypted in accordance with the Federal Information Processing Standards (FIPS) Publication 140-2. Vendor shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while Vendor has responsibility for the Protected Information under the terms of this Appendix.

B.E. PUBLISHING

ARTICLE 5 – RETURN OR DESTRUCTION OF PROTECTED INFORMATION

Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, Vendor shall return and destroy the District's Protected Information. This provision shall also apply to all Protected Information that is in the possession of subcontractors or agents of Vendor. Such destruction shall be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Vendor shall certify in writing to District that such return or destruction has been completed.

ARTICLE 6 – BREACHES OF PROTECTED INFORMATION

A. **Definition**. For purposes of this article, a "Breach" has the meaning given to it under relevant California or federal law, for example, California Civil Code Section 1798.29, California Health and Safety Code Section 1280.15, etc.

B. **Reporting of Breach**: Vendor shall report any confirmed or suspected Breach to District immediately upon discovery, both orally and in writing, but in no event more than two (2) business days after Vendor reasonably believes a Breach has or may have occurred. Vendor's report shall identify: (i) the nature of the unauthorized access, use or disclosure, (ii) the Protected Information accessed, used or disclosed, (iii) the person(s) who accessed, used and disclosed and/or received Protected Information (if known), (iv) what Vendor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (v) what corrective action Vendor has taken or will take to prevent future unauthorized access, use or disclosure. Vendor shall provide such other information, including a written report, as reasonably requested by District. In the event of a suspected Breach, Vendor shall keep the District informed regularly of the progress of its investigation until the uncertainty is resolved.

C. **Coordination of Breach Response Activities**: In the event of a Breach, Vendor will:

1. Immediately preserve any potential forensic evidence relating to the breach, and remedy the breach as quickly as circumstances permit;
2. Promptly (within 2 business days) designate a contact person to whom the District will direct inquiries, and who will communicate Vendor responses to District inquiries;
3. As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore District service(s) as directed by the District, and undertake appropriate response activities;
4. Provide status reports to the District on Breach response activities, either on a daily basis or a frequency approved by the District;
5. Coordinate all media, law enforcement, or other Breach notifications with the District in advance of such notification(s), unless expressly prohibited by law;
6. Make all reasonable efforts to assist and cooperate with the District in its Breach response efforts; and
7. Ensure that knowledgeable Vendor staff are available on short notice, if needed, to participate in District -initiated meetings and/or conference calls regarding the Breach.

D. **Costs Arising from Breach**. In the event of a Breach, Vendor agrees to promptly reimburse all costs to the District arising from such Breach, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of District personnel responding to Breach, civil or criminal penalties levied against the District, attorneys fees, court costs, etc. Any Breach may be grounds for immediate termination of this Agreement by the District.

ARTICLE 7 – EXAMINATION OF RECORDS

District and, if the applicable law, contract or grant so provides, the other contracting party or grantor (and if that be the United States, or an agency or instrumentality thereof, then the Controller General of the United States) shall have access to and the right to examine any pertinent books, documents, papers, and records of Vendor involving transactions and work related to this Appendix until the expiration of five years after final payment hereunder. Vendor shall retain project records for a period of five years from the date of final payment.

ARTICLE 8 – ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

Vendor shall make itself and any employees, subcontractors, or agents assisting Vendor in the performance of its obligations under the Agreement available to District at no cost to District to testify as witnesses, or otherwise, in the event of an unauthorized disclosure caused by vendor that results in litigation or administrative proceedings against District, its directors, officers, agents or employees based upon a claimed violation of laws relating to security and privacy and arising out of this Appendix.

ARTICLE 9 – NO THIRD-PARTY RIGHTS

Nothing in this Appendix is intended to make any person or entity that is not signatory to the Agreement a third-party beneficiary of any right created by this Appendix or by operation of law.

ARTICLE 10 – ATTORNEY'S FEES

In any action brought by a party to enforce the terms of this Appendix, the prevailing party shall be entitled to reasonable attorney's fees and costs, including the reasonable value of any services provided by in-house counsel. The reasonable value of services provided by in-house counsel shall be calculated by applying an hourly rate commensurate with prevailing market rates charged by attorneys in private practice for such services.

ARTICLE 11 – INDEMNITY

Vendor shall indemnify, defend and hold District (and its officers, directors, agents and employees) harmless from all lawsuits, claims, liabilities, damages, settlements, or judgments, including District's costs and attorney fees, which arise as a result of Vendor's negligent acts or omissions or willful misconduct.

ARTICLE 12 – SURVIVAL

The terms and conditions set forth in this Appendix shall survive termination of the Agreement between the parties. If Vendor is unable to return or destroy the District's Protected Information in accordance with Article 6, then this Appendix, in its entirety, shall survive the Agreement until such time as Vendor does return or destroy the Protected Information.

ARTICLE 13 - REGULATORY COMPLIANCE CHECKLIST

The procedures on Exhibit A are to be adhered to by all vendor representatives at all times.

Vendor has all requisite power and authority to conduct its business and to execute, deliver, and perform the Agreement. Each party warrants that the individuals who have signed this Agreement have the legal power, right, and authority to make this Agreement and bind each respective party.

IN WITNESS THEREOF, the parties hereto have executed this Agreement on the date written below:

Jurupa Unified School District:

____
Authorized Signature

Jeffrey Lewis
Type or print name

Director, CSS
Title

____
Date

Vendor:

Authorized Signature

Rennie M Sullivan
Type or print name

Director of Business Operations
Title

9/22/17
Date

B.E. Publishing, Inc.
Business Name

Exhibit A - Data Security and Privacy Agreement for FY 17/18 (July 1, 2017-June 30, 2018)

Section I: General (All data)

1. PASSWORD SECURITY. All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Jurupa USD Education-Information Technology ("TECHNOLOGY") management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. Jurupa Unified School District "District" personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by TECHNOLOGY management.
   Agree: Yes__X__No _______

2. SYSTEM SECURITY. Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware and software is prohibited.
   Agree: Yes__X__No _______

3. PRIVACY. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and District policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by TECHNOLOGY management and state and federal law.
   Agree: Yes__X__No _______

4. REUSE: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Jurupa Unified School District data without the prior, written consent of TECHNOLOGY Branch management.
   Agree: Yes__X__No _______

5. TRANSPORT: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc.) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.
   Agree: Yes__X__No _______

6. EXTERNAL SECURITY: *Vendor must attach to this document* reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.
   Agree: Yes__X__No _______

7. INTERNAL SECURITY: *Vendors must attach to this document* reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personnel (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?
   Agree: Yes__X__No _______

8. DISTRICT ACCESS: Vendor must provide a secure means (see Item 6 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor provided extract as needed by the District (not to exceed quarterly). *Describe the means and format of the data* (delimited, Excel, MDB, SQL Dump).
   Agree: Yes__X__No _______

9. TERMINATION: Upon termination of an executed contract with the District as provided herein, vendor will permanently delete all customer data from their system as allowed by state and federal law.
   Agree: Yes__X__No _______

Section II: AB1584 Compliance (Student information only)

1. Vendor agrees that the Jurupa Unified School District retains ownership and control of all student data.
   Agree: Yes__X__No_______N/A _______

2. *Vendor must attach to this document* a description of how student created content can be exported and/or transferred to a personal account.
   Agree: Yes_______No_______N/A __X__

3. Vendor is prohibited from allowing third-parties use of student information beyond those purposes defined in an executed contract with the District.
   Agree: Yes__X__No_______N/A _______

4. *Vendor must attach to this document* a description of how parents, legal guardians and students can review and correct their personally identifiable information.
   Agree: Yes__X__No_______N/A _______

5. *Vendor will attach to this document* evidence, including designation and training, of how student data is kept secure and confidential, including third-party access.
   Agree: Yes__X__No_______N/A _______

6. *Vendor will attach to this document* a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
   Agree: Yes__X__No_______N/A _______

7. Vendor certifies that student records will not be retained or available to a third party once the District contract has expired or is canceled. *Vendor will attach to this document* a description of how that certification is enforced
   Agree: Yes__X__No_______N/A _______

8. *Vendor will attach to this document* a description of how they and any third party affiliates comply with FERPA.
   Agree: Yes__X__No_______N/A _______

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students.
   Agree: Yes__X__No_______N/A _______

Section III: SB 1177 SOPIPA Compliance (Student information only)

1. Vendors cannot target advertising on their website or any other website using information acquired from students.
   Agree: Yes__X__No_______N/A _______

2. Vendors cannot create a profile for a student except for school purposes as defined in the an executed contract with the District.
   Agree: Yes__X__No_______N/A _______

3. Vendors cannot sell student information.
   Agree: Yes__X__No_______N/A _______

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.
   Agree: Yes__X__No_______N/A _______

5. *Vendors must attach to this document* evidence of how student information is protected through reasonable security procedures and practices.
   Agree: Yes__X__No_______N/A _______

6. Vendors must delete district-controlled student information when requested by the Jurupa Unified School District.
   Agree: Yes__X__No________N/A _______

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.
   Agree: Yes__X__No________N/A _______

Exhibits (attach additional sheets as needed)

Section I.6 External Security:

EduTyping has an industry-standard AWS private cloud. All backend systems have security layers both intrinsic in the design and applied as a layer. All backend systems are only accessible via the corporate network.

The corporate network is secured using:

- Private VPC without public IP on backend systems thereby making internet-to-instance traffic impossible.
- Private servers and services are access only when connected to the corporate VPN.
- Production tier systems are only accessible to primary stakeholders.
- Encryption occurs at the CloudFlare endpoint.
- Public services are provided through product-specific, dedicated ELB's, only across HTTPS.
- All services are "wrapped" in atomic, discreet security groups (AWS firewall implementation).
- All behind VPN.
- SSH with hostkeys.
- Hostkey-per-user.
- No IDS.
- STAGE/DEV systems have the same security as production with additional internal development team access.

Section I.7 Internal Security:

- All Operations team members have access to all data.
- Vendor personnel do not have access to District data, or processing systems, or backups.
- Data enters the API and is stored in the database.
- Database is secured using non-shared credentials that are stored in encrypted version control.
- Backups are performed nightly and are full snapshots, and only employees specifically granted atomic access to databases and/or backups..
- Backups are nightly, and stored for a week.
- There is no backup media outside of cloud-storage in AWS datacenter only.
- Backups are purged and overwritten by AWS.
- Data is rarely printed. In the event data is printed, it is disposed of normally.

Section I.8 District Access:

- EduTyping uses its own API based authentication, authorization, and transport (Rest).
- Database dumps can be made available.

Section II.2 Exporting of student created content:

EduTyping does not provide the capability for a student to transfer their content data out of the system.

Section II.4 Review and correcting personally identifiable information:

If granted by the teacher (via EduTyping application preferences), students may be allowed to change their First Name, Last Name, and Password. Note that student names are not required in EduTyping (just a username and password are req'd) and are only entered if desired by the teacher, school, or district. Parents/Guardians may coordinate with the teacher/school/district for making changes.

Section II.5 Securing student data:

All student-related content is password-protected and only accessible by administrators or teachers associated with the student.

B.E. Publishing staff is trained annually on how to insure student data is kept secure. Last staff training was conducted on September 22, 2017. 3rd party access is not allowed with the exception of our Single Sign-On service provider (Clever) who must themselves comply with student data privacy agreements via our contract agreement with them.

Section II.6 Disclosure notification:

B.E. Publishing (EduTyping) does not collect contact information for a student's parent, legal guardian, or an eligible student so direct notification by B.E. Publishing would not be possible. In the unlikely event of an unauthorized disclosure of student account information, B.E. Publishing will notify the school/district administrator.

Section II.7 Destruction of records:

B.E. Publishing (EduTyping) does not remove/delete student records. It is the responsibility of the school/district account administrator to remove student data upon completion of the expiration or cancellation of the account.

Section II.8 FERPA compliance:

B.E. Publishing (EduTyping) complies with FERPA by insuring that student records within EduTyping are under the complete and direct control of the school/district at all times. Further, B.E. Publishing also certifies compliance with school/district student privacy requirements that are themselves designed to insure FERPA compliance by the school/district.

Section III.5 How student data is protected:

B.E. Publishing employs technology, procedures, and staff training to insure student data is protected at all times.