

# DATA PRIVACY AGREEMENT

## Lancaster Central School District

This Data Privacy Agreement ("DPA") is by and between the **Lancaster Central School District** ("EA"), an Educational Agency, and Emotional ABCs  
("Contractor"), collectively, the "Parties".

### ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency (EA):** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.

- 10. Personally Identifiable Information (PII):** Means student personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.
- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable student information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 15. Subcontractor:** Contractor’s non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

## **ARTICLE II: PRIVACY AND SECURITY OF PII**

### **1. Compliance with Law**

In order for Contractor to provide certain services ("Services") to the EA pursuant to date services begin 5/16/2022 [date agreement is signed will populate upon signature]; Contractor may receive PII regulated by applicable New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education’s Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

### **2. Authorized Use**

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in this DPA. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

### **3. Data Security and Privacy Plan**

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

### **4. EA's Data Security and Privacy Policy**

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework.

### **5. Contractor's Employees and Subcontractors**

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to this DPA where the subcontractor will receive or have access to PII are consistent with those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees.
- (e) Contractor must not disclose PII to any unauthorized party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

### **6. Training**

To the extent required by law, the contractor shall ensure that all its employees and subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

### **7. Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its subcontractors retain PII or retain access to PII pursuant to the service agreement. Contractor will automatically delete all PII from its servers after a period of two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks. The EA may use the administrator portal to delete all PII at any time or may request assistance from Contractor to delete PII at any time. The confidentiality and data security

obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon deletion of PII from both active servers and backups.

#### **8. Data Return and Destruction of Data**

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period prescribed by this agreement, or as expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. The EA may use the administrator portal to delete PII at any time or may request assistance from Contractor to do so. If not deleted by the EA, Contractor will automatically delete all PII from its servers after a period of no more than two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks.
- (b) With regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Upon request, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data.

#### **9. Commercial or Marketing Use Prohibition**

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose, except that teachers may receive email communications regarding product updates or professional development opportunities from which they may opt out at any time.

#### **10. Encryption**

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

#### **11. Breach**

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified mail, and must to the extent available, include a description of the Breach which

includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Michele Ziegler,  
Data Protection Officer/Director of Instructional Technology and Accountability  
Lancaster Central School District  
177 Central Avenue  
Lancaster, NY 14086  
[mziegler@lancasterschools.org](mailto:mziegler@lancasterschools.org)

## **12. Cooperation with Investigations**

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach of data governed by this DPA.

## **13. Notification to Individuals**

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full actual cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

# **ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS**

## **1. Parent and Eligible Student Access**

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to this DPA, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to this DPA, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

## **2. Bill of Rights for Data Privacy and Security**

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for this DPA are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.


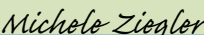
## ARTICLE IV: MISCELLANEOUS

### 1. Priority of Agreements and Precedence

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

### 2. Execution

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

<b>Contractor Name:</b> Emotional ABCs	
<b>Signature:</b>	 <small>Ross Brodie (May 16, 2022 09:01 PDT)</small>
<b>Printed Name:</b>	Ross Brodie
<b>Title:</b>	CEO
<b>Email:</b>	Support@EmotionalABCs.com
<b>Date:</b>	5/16/2022
<b>Lancaster Central School District Data Protection Officer – Michele Ziegler</b>	
<b>Date:</b> May 16, 2022	<b>Signature:</b>  <small>Michele Ziegler (May 16, 2022 14:59 EDT)</small>

## **EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security**

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following

### **PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

The Lancaster Central School District is committed to protecting the privacy and security of student protected data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

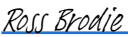
1. A student's personally identifiable information cannot be sold or released for any commercial purpose.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices including, but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student protected data elements collected by New York State (<http://www.nysed.gov/data-privacy-security/student-data-inventory>) is available for public review or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student protected data or teacher or principal Annual Professional Performance Review data. Any such complaint must be submitted, in writing, to: Michele Ziegler, Director of Instructional Technology, 177 Central Avenue, Lancaster, New York 14086. Additionally, parents have the right to have complaints about possible breaches of student protected data addressed. Complaints should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234; the email address is "cpo@mail.nysed.gov". The State Education Department's complaint process is under development and will be established through regulations from the department's chief privacy officer, who has yet to be appointed.

### **Supplemental Information Regarding Third-Party Contractors**

In the course of complying with its obligations under the law and providing educational services to District residents, the Lancaster Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., Family Educational Rights and Privacy Act; Education Law Section 2-d);
3. The duration of the contract, including the contract’s expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to protect the data privacy and mitigate security risks; and
6. Address how the data will be protected using encryption while in motion and at rest.

<b>Contractor Name:</b> Emotional ABCs	
<b>Signature:</b>	 <small>Ross Brodie (May 16, 2022 09:01 PDT)</small>
<b>Printed Name:</b>	Ross Brodie
<b>Title:</b>	CEO
<b>Email:</b>	Support@EmotionalABCs.com
<b>Date:</b>	5/16/2022



## EXHIBIT B – Bill of Rights for Data Privacy and Security

### Supplemental Information for Contracts That Utilize Personally Identifiable Information

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	<b>The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the district with functionality of the product or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.</b>
<b>Type of PII that Contractor will receive/access</b>	Check applicable options: <input checked="" type="radio"/> Student PII <input type="radio"/> BOTH Student PII and APPR Data <input type="radio"/> APPR Data
<b>Contract Term</b>	Start Date: <u>5/16/2022</u>  End Date: Agreement remains in effect as long as the account is current and in good standing or upon expiration of the master agreement without renewal, or upon termination of the master agreement prior to its expiration.
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option)  <input type="radio"/> Contractor will not utilize subcontractors. <input checked="" type="radio"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall:  <input type="radio"/> Securely transfer PII to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties.  <input checked="" type="radio"/> Securely delete and destroy PII.
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify the Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.
<b>Secure Storage and Data Security</b>	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)  <input checked="" type="radio"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="radio"/> Using Contractor owned and hosted solution <input type="radio"/> Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

## EXHIBIT B – Bill of Rights for Data Privacy and Security

<b>Contractor Name:</b> Emotional ABCs	
<b>Signature:</b>	<u><i>Ross Brodie</i></u> <small>Ross Brodie (May 16, 2022 09:01 PDT)</small>
<b>Printed Name:</b>	Ross Brodie
<b>Title:</b>	CEO
<b>Email:</b>	Support@EmotionalABCs.com
<b>Date:</b>	5/16/2022

## EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. **For every contract, the Contractor must review the following list and provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State.**

### CONTRACTORS ATTACHED PLAN SHALL INCLUDE THE FOLLOWING:

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.
7	Describe your secure destruction practices and how certification will be provided to the EA.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 <a href="https://www.nist.gov/cyberframework/new-framework">https://www.nist.gov/cyberframework/new-framework</a>



# Privacy Policy

Emotional ABCs, Inc. (hereafter “Company”) has adopted the following Privacy Policy applicable to all visitors or users of this website ("Users"). Users who do not agree with the terms of this Privacy Policy should immediately exit the website.

## 1. TYPES OF DATA COLLECTED AND PROCESSED.

Company stores and processes the information Company collects in the United States in accordance with this Privacy Statement. Company's sub-processors may store and process data outside the United States. User data collected on the site includes the User's name, address, e-mail addresses, credit card information, order information, browser type, and the date and time of each User request. Company also collects potentially personally-identifying information like Internet Protocol (IP) addresses, and any other information voluntarily provided (hereafter "Personal Information"). Company understands that Users may be from different countries and regions with different privacy laws and expectations, and Company tries to meet or exceed those expectations even when the United States may not have the same privacy regulations as other countries. Company provides the same standard of privacy protection — as described in this Privacy Statement — to all Users around the world, regardless of their country of origin or location. Company strives to implement and adhere to the strictest standards of notice, choice, accountability, security, data integrity, access and recourse practically available. Company's vendors or User's school or educational institutions that have access to User Personal Information are also required to maintain the security and integrity of any User Personal Information. Company provides clear methods of unambiguous, informed consent at the time of data collection, when Company collects User's Personal Information using consent as a basis. Company collects only the minimum amount of Personal Information necessary for Company's purposes unless Users choose to provide more. Company offers Users simple methods of accessing, correcting, or deleting the User Personal Information collected by Company. Company provides Users notice, choice, accountability, security, and access, and limits the purpose for processing. Company also provides Users a method of recourse and enforcement. Company collects and stores Personal Information about Users of the site on third party servers to enable transactions and for site security and analytics.

Company may collect and store Personal Information or other data about patterns of usage and order history; which activities a User starts and finishes; when the User starts and stops an activity, and which areas of the site a User visits. Only Personal Information or other data necessary to the operation, maintenance, and improvement of Company's business is collected.

Names of Users or children on Unit completion Certificates do not include last names or any other identifying information. Similarly, User's or children's names and passwords within the website only include first names, avatars, and picture passwords. No last names or other information is collected or stored by Company other than in connection with credit card payment information including first and last names of credit card holder, card number, expiration date, CCV number and billing address. Also, the website does not require the full name or age or any other information about any User or child. Only information of the parent, guardian or other individual over the age of 18 using a credit card to register at the website is taken by Company. Only a first or nickname for a child's log in information is required. Company collects and stores the following data: On Paid Family or Individual accounts: parent emails and passwords, all credit card related payment data, child username and picture password. On Free Parent accounts: parent emails and passwords, child username and picture password. On Free Teacher accounts: teacher email address and password, school and headmaster name, address, and phone number. On Paid Premium Classroom accounts: school email address and password, school name and other school identifying information, and all credit card related payment data, student rosters with student's first name and first three letters of student's last name, parent's email address once input by the school, and parent password once a parent has agreed to sign up for program use at home. During the course of providing the service, Company also collects information about the Users use of the service and information submitted such as progress within the consecutive learning program for the purpose of awarding online and printable certificates to the students at the end of each unit.

Premium Classroom account holders represent and warrant that they have obtained written permission and consent for the student to use the service from the student user's parent or legal guardian. Users may review this data and request it be removed or corrected by contacting Company's webmaster at: [Privacy@EmotionalABCs.com](mailto:Privacy@EmotionalABCs.com). Company is not responsible for, and has no control over, Personal Information or other data collected by Schools or provided by Users to Schools or other third parties.

## 2. STUDENT PRIVACY PLEDGE

Company adheres to the Student Privacy Pledge, an industry standard approach to privacy for K-12 service providers ("The Pledge"). The Pledge was created by the Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA) and has been endorsed by the National School Boards Association (NSBA), the National Parent-Teacher Association (PTA), and the White House.

As part of Company's commitment to The Pledge, when Company has access to User or student Personal Information through the provision of Company's

Services, the following principles guide Company's practices regarding data, security, and technology:

Company commits to:

- Not collect, maintain, use or share student Personal Information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.
- Not sell student Personal Information.
- Not use or disclose student information collected through an educational/school service (whether Personal Information or otherwise) for behavioral targeting of advertisements to students.
- Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student.
- Not make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data is used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student Personal Information that are inconsistent with contractual requirements.
- Not knowingly retain student Personal Information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student.

Company affirmatively commits to the following:

- Collect, use, share, and retain student Personal Information only for purposes authorized by the User, School, agency, teacher or parent/student.
- Disclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student Personal Information Company collects, if any, and the purposes for which the Personal Information Company maintains is used or shared with third parties.
- Support access to and correction of User/student personally identifiable information by the User/student or their authorized parent, either by assisting the School in meeting its requirements or directly when the information is collected directly from the User/student with student/parent consent.
- Maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of User/student Personal Information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of

administrative, technological, and physical safeguards appropriate to the sensitivity of the information.

- Provide resources to support educational institutions/agencies, teachers, or parents/students to protect the security and privacy of student Personal Information while using the educational service.
- Require that Company's vendors with whom student Personal Information is shared in order to deliver Company's educational services, if any, are obligated to implement these same commitments for the given User/student Personal Information.
- Allow a successor entity to maintain the student/User Personal Information, in the case of Company's merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student Personal Information.
- Incorporate privacy and security when developing or improving our educational products, tools, and services and comply with applicable laws.

### 3. CROSS-BORDER DATA TRANSFERS

For cross-border data transfers from the European Union (EU) and the European Economic Area (EEA), Canada or Australia, in addition to providing Users methods of unambiguous, informed consent and control over their data, Company is committed to subject any Personal Information received from the EU, EEA, Australia, Canada or anywhere else to the same stringent protections and limitations. Company adheres to the federal privacy protection standards in the Children's Online Privacy Protection Act (COPPA), the California Online Privacy Protection Act of 2003 ("CalOPPA"), the Student Privacy Pledge, the Family Educational Rights and Privacy Act ("FERPA"), The Student Online Personal Information Protection Act ("SOPIPA"), California Assembly Bill 1584 ("AB 1584") and the California Consumer Privacy Act ("CCPA" - AB 375). Further, Company uses reasonable efforts to comply with the General Data Protection Regulation ("GDPR"), the Canadian Personal Information Protection and Electronic Documents Act ("PipEDA"), the Australian Commonwealth Privacy Act, and other applicable laws, statutes, regulations and treaties worldwide. Company does not intentionally collect Personal Information online from children without their parent's consent other than as described herein. Children may visit any area of the site and may participate in activities without providing any Personal Information or other data. Online orders, however, may only be placed by adults over the age of 18 or by minors under the age of 18 with the consent of the minor's parent or legal guardian. In authorizing persons under 18 to place orders through the site, the parent or legal guardian consents to the collection of Personal Information or other data necessary to process and complete the transaction and for security purposes. If a person under 18 sends a request to Company, Company webmaster will keep their e-mail address for long enough to respond to them. Company may delete this information from its system in the ordinary course of business, generally after the question is answered. Parents may request to review or delete any information submitted by his or her child by

sending an email to Company's webmaster at "Privacy@EmotionalABCs.com" or by sending a written, postpaid request addressed to: Emotional ABCs, Inc., 3435 Ocean Park Blvd #107-259, Santa Monica, CA 90405-3300 - Attn: Webmaster, Children's Online Privacy Act - Delete Request. Requests must include proof verifying that the requester is the parent of the child whose information is requested.

#### 4. COOKIES, TRACKING

In addition to Personal Information, Company's web servers automatically identify computers by their IP addresses. Company may use IP addresses to administer the site or gather other information. Further, the site may use "cookies" during the session transaction process to enable ordering. By using Company's website, Users agree Company can place these types of cookies on User's computer or device. If User disables User's browser or device's ability to accept these types of cookies User will not be able to login or use Company's website services. Company currently does not respond to Users' browser's Do Not Track signal. Company does not permit third parties other than Company's analytics and service providers to track Users' activities on the site. Company does not track Users' online browsing activities on other online sites or services. Company does not disclose cookie data to any third party.

#### 5. USE OF DATA

Company may use Users' Personal Information to identify Users for online activities such as online ordering or any other online interactive activities, to respond to specific requests from Users, to obtain parental consent from Users under 18 years of age when necessary and to protect the security or integrity of the website.

#### 6. TYPE AND IDENTITY OF THIRD PARTIES TO WHOM DATA IS DISCLOSED

Company does not disclose the personally identifiable information of any User to third parties for any marketing or promotional purposes. Company may disclose de-identified and/or aggregated User information for any other purpose as permissible by applicable law—for example, the distribution of de-identified User records to outside researchers or the distribution of reports containing aggregate user demographic and traffic patterns—provided that no individual User or any specific end user device can be readily identified.

Company does not sell, rent, loan, transfer, or otherwise disclose any Personal Information to third parties except as set forth in this Privacy Policy. Company shares with third-party payment services (such as PayPal and its subsidiary companies) Users personal information related to credit card payments (cardholders first and last names, card number, expiration date, CCV code, and billing address) only to the extent necessary to process payment and for site



security. Company may also share Personal Information with third parties with or without notice to User in connection with a court order, subpoena, government investigation, when otherwise required by law. Subject to confidentiality agreements, the terms of this Privacy Policy and applicable law, Personal Information may be disclosed to service providers and advisors to support the website's technical operation or to execute a specific program. Any third parties with whom Personal Information is shared shall be bound by this Privacy Policy. Personal Information may also be shared with potential transactional partners or other third parties in connection with the consideration, negotiation, or completion of a corporate transaction in which Company is sold in whole or part to, acquired by, or merged with, another entity, or Company sells, liquidates, transfers, or licenses all or a portion of Company's assets in bankruptcy or otherwise. If some or all of Company's assets are acquired or otherwise transferred or licensed, including in bankruptcy, the entity or person acquiring Company's assets shall be subject to the same commitments stated under this Privacy Policy. Certain data related to User Personal Information which data does not necessarily identify specific Users names, such as the length of interaction, volume and frequency of site activity, etc. may be stored and used by Company in connection with site analytics to understand and improve Company services, products and the User experience, detect security incidents, conduct research, prevent fraud, debug, repair errors, maintain Users account, provide user/customer service, activities to improve Company's services.

## 7. PURPOSES FOR WHICH DATA IS PROCESSED

Under certain international laws (including GDPR), Company is required to notify you about the legal basis on which we process User Personal Information. Company processes User Personal Information on the following legal bases: When Users create a Company account, Users provide username and an email address. Company requires those data elements for User to enter into the Terms of Service agreement with Company, and Company processes those elements on the basis of performing that contract. Company also processes Users' username and email address on other bases. Company does not collect or process a credit card number, but our third-party payment processor does.

Company does not permit children under the age of 13 to create an account and does not knowingly collect personally identifying information from children under the age of 13 without the consent and at the direction of a parent. Company permits parents to set up child profiles associated with the parent account so that the children may access the service under the parents' supervision. We take special precautions to collect only as much information as is reasonably necessary for the child to use the service and to ensure the parents have access to and control of their child use of the service. By creating a child profile associated with a parent account or permitting your child to use the Companies of service you expressly agree to the practices described in this Privacy Policy

and consent to the collection, use, and disclosure of your child's Personal Information as described herein.

On Individual or Family accounts, the parent uses the parent's own email, password and credit card information. Parents and children together create a username of their own choice and choose a picture password. Child Users require the parent's email and parent's password to begin using the service. On Free Teacher accounts, teachers get a single user account for themselves. Teachers use their own email address and password and create a single user account for themselves.

On Premium Classroom accounts teachers or administrators use their school email address and password and school related information when they sign up for the service. School administrators or teachers are able to add student rosters which include student first names in the first three letters of student last names but no other identifying information about students. Teachers assign students into their accounts with a QR code or a website link in the classroom. Parents get an email from the school or the teacher allowing them to sign into the Premium Classroom individual student account with the parents own email and password to allow the child/student to use their school account from home.

When Users fill out the information in User's user profile, Users have the option to provide User Personal Information such as User's full name, an avatar, and first name or nickname. Company processes this information on the basis of consent. All of this information is entirely optional, and Users have the ability to access, modify, and delete it at any time. Generally, the remainder of the processing of Personal Information by Company is necessary for the purposes of Company's legitimate interests. For example, for security purposes, Company must keep logs of IP addresses that access Company, and in order to respond to legal process, Company is required to keep records of users who have sent and received DMCA takedown notices. If you would like to request erasure of data we process on the basis of consent or object to our processing of Personal Information, Users or Parents of Users may request to review, correct or delete any information submitted by User or User's child by sending an email to Company webmaster at: "Privacy@EmotionalABCs.com" or a written request addressed to Emotional ABCs, Inc., 3435 Ocean Park Blvd #107-259, Santa Monica, CA 90405-3300 - Attn: Webmaster, Children's Online Privacy Act - Delete Request. Requests must include proof verifying that the requester is the User or parent of the child whose information is requested.

When Company changes or deletes any Personal Information at User's request, Company will make good faith efforts to make the changes in our then-active databases as soon as reasonably practicable, generally within 24–48 hours. Changing setting options may not result in immediate changes to the settings, which are subject to our operations and maintenance schedules. Please note that information may remain in backup or archive records, and Company may retain

certain data relevant to preventing fraud or future abuse or for legitimate business purposes, such as analysis of aggregated, non-personally-identifiable or de-identified data, account recovery, or if required by law. All retained data will continue to be subject to the Privacy Policy in effect at that time.

Upon Account cancellation, de-identified User Personal Information may nonetheless persist internally in Company's archive files or similar databases, and may still be used, on a de-identified basis, for Company's internal support, administrative, and record-keeping purposes including, but not limited to, allowing Company to improve its site and services and other services provided through research, evaluation, and analytics as permissible by applicable law. Please note that following a request to delete User Personal Information or other information including Personal Information may remain in backup or archive records, and Company may retain certain data if required by law, relevant to preventing fraud or future abuse, or for legitimate business purposes, such as account recovery and customer support, and all subject to our internal records retention periods. All retained data will continue to be subject to the Privacy Policy in effect at that time and applicable law.

Company will not retain Personal Information longer than necessary and will delete all student Personal Information at the termination of the contract or when it is no longer needed by Company.

## 8. SECURITY

Company uses appropriate physical, technical, and administrative security measures to protect and safeguard all Personal Information collected in a secure, controlled environment to which third parties are generally not permitted access. Other security safeguards include but are not limited to, data encryption, firewalls, and physical access controls to buildings and files. Company will notify affected Users if any User data is lost, stolen or compromised and will take all appropriate steps to avoid any further unauthorized disclosure or dissemination. No data transmissions over the internet can be guaranteed to be 100% secure. Consequently, Company cannot ensure or warrant the security of any information Users transmit to Company and Users agree to do so at their own risk. Company has multiple security measures in place to protect the loss, misuse or alteration of information under its control. This website is hosted in the United States. If you are visiting from the European Union or other regions with laws governing data collection and use that may differ from U.S. law, please note that you are transferring your personal data to the United States, which does not have the same data protection laws as the EU or other regions; by providing your personal data you consent to the use of your personal data for the uses identified above in accordance with this Privacy Policy and the transfer of your personal data to the United States as indicated above.

## 9. LINKING

This website may contain links to other websites that may not be owned or operated by Company. This Privacy Policy applies solely to Personal Information collected on this site. These links are provided for User's convenience to provide further information. They do not signify that Company endorses the website(s). Company has no responsibility for the content of the linked website(s). Company will only link to businesses that have privacy practices consistent with Company's Privacy Policy, or have agreed to be bound by Company's Privacy Policy.

## 10. PASSWORDS

Users to the website select a password to access the Materials and Content and other features of the website and allow Users to review and change the information Company collects about them or their child. Users' passwords should be kept confidential.

## 11. CHANGES TO PRIVACY POLICY

If you have any further questions concerning Company's Privacy Policy and the use of your Personal Information, please contact Company's webmaster at: "Support@EmotionalABCs.com". This Privacy Policy was last updated, and its Effective Date is June 21, 2021. Company will post any changes on the site's homepage. For certain other changes, including all material changes, to its Privacy Policy Company will give notice and obtain consent by either 1) displaying an alert and an "Agree" button next to the Privacy Policy, or 2) displaying an alert and an "Agree" button upon login, or 3) directly communicating with Users through the email address associated with the User account.

## 12. DISPUTE RESOLUTION

Company and User agree to all terms and conditions regarding dispute resolution and arbitration set forth in Company's Terms of Use, which terms and conditions are incorporated herein by reference.

## 13. (a) CALIFORNIA PRIVACY RIGHTS

This Section applies to the use of Company's service by Schools located in the State of California. This section documents compliance with applicable California state laws that may apply to the use of Company's service by Schools in California, such as the California Consumer Privacy Act, California Civil Code §§ 1798.100 et seq. ("CCPA"), California Online Privacy Protection Act of 2003 ("CalOPPA"), California Assembly Bill 1584 ("AB 1584"), and the California Consumer Privacy Act ("CCPA") - AB 375. Effective January 1, 2020, the California Consumer Privacy Act California Civil Code §§ 1798.100 et seq. ("CCPA") provides California residents with specific rights regarding their

**Personal Information.** This section describes User CCPA rights and explains how to exercise those rights. The CCPA can be reviewed at [oag.ca.gov/privacy/ccpa](http://oag.ca.gov/privacy/ccpa). In this section "User" or "Users" refers to California residents. Under the CCPA Company is required to disclose categories of sources from which Company collects Personal Information, and the third parties with whom Company shares such information. Company is also required to communicate information about rights Users have under California law, such as:

**Right to access Personal Information.** [CC § 1798.100] Users may be entitled to receive the specific pieces of User Personal Information Company holds.

**Right to data portability.** [CC § 1798.100] Users may be entitled to receive a copy of User electronic Personal Information in a readily usable format.

**Right to disclosure.** [CC §§1798.110, 1798.115] User may be entitled to receive information regarding the categories of Personal Information Company collected, the sources from which Company collected Personal Information, the purposes for which Company collected and shared Personal Information, the categories of Personal Information that Company sold, the categories of third parties to whom the Personal Information was sold, and the categories of Personal Information that Company disclosed for a business purpose in the 12 months preceding the User request. In the 12 months preceding January 1, 2020, Company did not disclose to any third party any categories of User Personal Information for business purposes or otherwise, including without limitation: identifiers, commercial information, electronic network and Internet activity information, geolocation data, or inferences about Users drawn from such data.

**Right to deletion.** [CC § 1798.105] Users may be entitled to request that Company delete the Personal Information that Company has collected from User. Company will use commercially reasonable efforts to honor User requests in compliance with applicable laws. Please note, however, Company may need or be required to keep such information, such as for Company's legitimate business purposes or to comply with applicable law.

**Right to opt-out of certain sharing with third parties.** [CC § 1798.120] Users are entitled to direct Company to stop disclosing User Personal Information to third parties for monetary or other valuable consideration. Company does not currently disclose any User Personal Information to any third parties for monetary or other valuable consideration. If Company ever does disclose any User Personal Information to third parties, Users can exercise such right to opt-out by clicking on the link on Company's homepage titled "Do Not Sell My Personal Information," which will direct Users to an Internet Company page that enables Users, or a person authorized by the User, to opt-out of the sale of the User's Personal Information. Company does not require a User or consumer to create an account in order to direct Company not to sell the User's/consumer's Personal Information. User/consumers can also opt-out by sending an email to Company's



webmaster at [Support@EmotionalABCs.com](mailto:Support@EmotionalABCs.com), sending a written, postpaid request addressed to: Emotional ABCs, Inc., 3435 Ocean Park Blvd #107-259, Santa Monica, CA 90405-3300- Attn: Company webmaster, or by calling toll-free (877) 399-8763.

Company will never monetize User Personal Information by providing it to a third party in exchange for money. The CCPA has a broader definition of the term "sell" which includes disclosing Personal Information to any third party for valuable consideration. Company does not share any Personal Information with any of Company's advertising partners, nor does Company disclose any of its cookie data to any third parties.

In addition, Company is required to provide User certain information about the business and commercial purposes for which Company collects and shares User Personal Information. Company may use or disclose User Personal Information Company collect for the business purposes described in this policy, including but not limited to: processing payments, conducting research, detecting security incidents, preventing fraud, debugging and repairing errors, maintaining User account, providing customer service, and other activities to improve Company's service, market Company's services, and understand how Users interact with Company's services. Non-Discrimination. [CC § 1798.125] Company fully supports User privacy rights and will not discriminate against Users for exercising any of User CCPA rights.

#### Exercising Access, Disclosure, Data Portability, and Deletion Rights

To exercise the access, disclosure, data portability, and deletion rights described above, please submit a verifiable consumer request by either contacting Company by email to Company's webmaster at [Privacy@EmotionalABCs.com](mailto:Privacy@EmotionalABCs.com), or send a postpaid written, request addressed: to Emotional ABCs, Inc., 3435 Ocean Park Blvd #107-259, Santa Monica, CA 90405-3300 - Attn: Webmaster, or by calling toll-free: (877) 399-8763.

#### Privacy Portal

Only a User or a person registered with the California Secretary of State that User has authorized to act on User's behalf may make a verifiable consumer request related to User Personal Information. Users may also make a verifiable consumer request on behalf of User's child.

Users may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must: i) Provide sufficient information to allow Company to reasonably verify User is the person about whom Company collected Personal Information or an authorized representative of User; and ii) describe User's request with sufficient detail to allow Company to properly understand, evaluate, and respond to it.

Company cannot respond to User requests or provide Users with Personal Information if Company cannot verify User's identity or authority to make the request and confirm the Personal Information relates to User. Making a verifiable consumer request does not require Users to create an account with Company. Company will only use Personal Information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

### 13. (b) CONNECTICUT PRIVACY LAWS

This Section applies to the use of Company's service by Schools located in the State of Connecticut. This section documents compliance with Connecticut state laws that may apply to the use of Company's service by Schools in Connecticut, such as Conn. Gen. Stat. Ann. § 10-234aa-dd, and incorporates by reference the definitions set forth in Conn. Gen. Stat. Ann. § 10-234aa.

If you open a Company account to provide the service to students in a School located in the State of Connecticut, you represent and warrant that you are authorized to do so on behalf of the local or regional board of education with authority over the School and that you are authorized to communicate with Company on behalf of the local or regional board of education.

Company and you shall comply with all applicable sections of Conn. Gen. Stat. Ann. § 10-234aa-dd. The following terms shall apply as required by Conn. Gen. Stat. Ann. § 10-234bb. To the extent that any such required terms conflict with other terms in this Agreement, the terms of this Section shall apply.

Student information, student records and student-generated content are not the property of or under the control of Company.

The local or regional board of education may request the deletion of any student information, student records or student-generated content in the possession of Company by sending a request to [Privacy@EmotionalABCs.com](mailto:Privacy@EmotionalABCs.com). As permitted by Conn. Gen. Stat. Ann. § 10-234bb(2), Company is not required to delete information prohibited from deletion or required to be retained under state or federal law or stored as a copy as part of a disaster recovery storage system and that is (i) inaccessible to the public, and (ii) unable to be used in the normal course of business by the contractor. Company will, however, comply with requests for deletion of student information, student records, or student-generated content that is restored from such disaster recovery storage systems.

Company will not use student information, student records and student-generated content for any purposes other than those authorized pursuant to this Agreement.

A student, parent or legal guardian of a student may review personally identifiable information contained in student information, student records or

student-generated content and correct erroneous information, if any, in such student record by contacting their School. Company will respond to such requests in accordance with instructions sent by an authorized School representative to [Privacy@EmotionalABCs.com](mailto:Privacy@EmotionalABCs.com).

Company will take actions designed to ensure the security and confidentiality of student information, student records and student-generated content.

Company will promptly notify the local or regional board of education in accordance with the provisions of section 10-234dd when there has been an unauthorized release, disclosure or acquisition of student information, student records or student-generated content.

Student information, student records or student-generated content shall not be retained or available to Company upon expiration of this Agreement. This restriction shall not apply to the extent that a student, parent or legal guardian of a student independently establishes or maintains an electronic account with Company for the purpose of storing their student-generated content.

Company and the local or regional board of education shall ensure compliance with the Family Educational Rights and Privacy Act of 1974, 20 USC §1232g, as amended from time to time.

The laws of the state of Connecticut shall govern the rights and duties of Company and the local or regional board of education.

If any provision of this Section is held invalid by a court of competent jurisdiction, the invalidity does not affect other provisions or applications of the contract which can be given effect without the invalid provision or application.

### 13. (c) NEW YORK PRIVACY LAWS

This Section applies to the use of Company's service by Schools located in the State of New York. This section documents compliance with applicable New York state laws that may apply to the use of Company's service by Schools in New York, such as New York State Education Law Section 2-d (Ed Law 2-d) and Part 121 of Title 8 of the Codes, Rules and Regulations of the State of New York (8 CRR-NY § 121) and incorporates by reference the definitions set forth in Ed Law 2-d § 3 and 8 CRR-NY § 121.1.

If you open a Company account to provide the service to students in a School located in the State of New York, you represent and warrant that you are authorized to do so on behalf of the educational agency with authority over the School and that you are authorized to communicate with Company on behalf of the educational agency.



Company and you shall comply with all applicable sections of Ed Law 2-d and 8 CRR-NY § 121. The following terms shall apply as required by Ed Law 2-d § 5(b)(3) and 8 CRR-NY § 121.3, 121.6. To the extent that any such required terms conflict with other terms in this Agreement, the terms of this Section 5.2 shall apply.

8 CRR-NY § 121.6(a)(1): outline how the third-party contractor will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy –

Company has implemented policies and procedures consistent with the New York State Education Department Data Privacy and Security Policy v1.0. It is the School's responsibility to provide Company with its data security and privacy policy if different than the New York State Education Department Data Privacy and Security Policy. Company will review its policies and procedures against data security and privacy policies provided to it by educational agencies. In the event Company's policies and practices are not consistent with the educational agencies' policies, Company will take commercially reasonable efforts to achieve consistency.

8 CRR-NY § 121.6(a)(2): specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract –

Company employs reasonable organizational and technical safeguards to prevent unauthorized access, use, alteration, or disclosure of personally identifiable information stored on systems under Company's control. Please see Section 8 of Company's Privacy Policy. School administrators may also request a copy of Company's Security Policies and Procedures.

8 CRR-NY § 121.6(a)(3): demonstrate that it complies with the requirements of section 121.3(c) of this Part –

The Parent Bill of Rights, along with any other supplemental documentation relating specifically to your School, is included in this contract unless Company and your School or District have entered into a separate signed written agreement regarding that subject matter. If your School does not have a Parent Bill of Rights, the New York State Parent Bill of Rights is applicable and is included in this contract.

8 CRR-NY § 121.3(c)(1) the exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract –

To provide the Company service as set forth in this Agreement. Student data and teacher or principal data will not be used for any other purpose.

8 CRR-NY § 121.3(c)(2) how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., FERPA; Education Law section 2-d) –

Subcontractors and other authorized persons or entities will be provided such information pursuant to contractual obligations to maintain the confidentiality of such data in a manner consistent with this Agreement.

8 CRR-NY § 121.3(c)(3) the duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed) –

This Agreement will be in effect for a School so long as that School has an active subscription to the Company service. Upon expiration or termination of a School's subscriptions without renewal, Company will delete student data and teacher or principal data in accordance with the terms of any applicable written agreement with the School, written requests from authorized School administrators, and our standard data retention schedule. Authorized School administrators may contact Company at [Privacy@EmotionalABCs.com](mailto:Privacy@EmotionalABCs.com). to request additional information about our standard data retention schedule and available options for customizing Company's standard data retention schedule to meet individual School requirements.

8 CRR-NY § 121.3(c)(4) if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected –

Parents, students, eligible students, and teachers or principals may contact their School to exercise this right. Company will cooperate with the School to effectuate such requests at the School's direction.

8 CRR-NY § 121.3(c)(5) where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated –

Student data and teacher or principal data for Schools located in New York will be stored in the United States. Such data will be stored in a manner consistent with the NIST Cybersecurity Framework to mitigate against data security and privacy risks.

8 CRR-NY § 121.3(c)(6) address how the data will be protected using encryption while in motion and at rest –

Company will utilize a technology or methodology specified or permitted by the Secretary of the United States Department of Health and Human services in guidance issued under section 13402(H)(2) of Public Law 111-5.

8 CRR-NY § 121.6(a)(4) specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the Federal and State laws governing confidentiality of such data prior to receiving access –

Company periodically provides training to its employees regarding data security and privacy obligations with respect to such data.

8 CRR-NY § 121.6(a)(5) specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected –

While Company does not sub-contract portions of any particular contract with a customer, Company may utilize vendors in the course of providing the Company service. Such vendors will only be provided personally identifiable information to the extent necessary for them to provide their contracted-for services and will be subject to obligations of confidentiality and security consistent with this Section.

8 CRR-NY § 121.6(a)(6) specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency –

Company will manage and respond to Security Events as set forth in Section 8 of this Privacy Policy. As required by Ed Law 2-d, Company will notify the school of a Security Event in the most expedient way possible and without unreasonable delay.

8 CRR-NY § 121.6(a)(7) describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires –

Upon expiration or termination of a School's subscriptions without renewal, Company will delete student data and teacher or principal data in accordance with the terms of any applicable written agreement with the School, written requests from authorized School administrators, and our standard data retention schedule. Authorized School administrators may contact Company at [Privacy@EmotionalABCs.com](mailto:Privacy@EmotionalABCs.com) to request additional information about our

standard data retention schedule and available options for customizing Company's standard data retention schedule to meet individual School requirements.

Last Updated: August 25, 2021