MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT
VERSION (2018)

Cambridge Public Schools

and

Cisco Systems, Inc.

December 12, 2018
This Massachusetts Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Cambridge Public Schools (hereinafter referred to as "LEA") and Cisco Systems, Inc. and its Affiliates (hereinafter referred to as "Provider") on the date of the last signature. The Parties agree to the terms as stated herein.

RECATALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain cloud security services and related maintenance and support services (collectively, "Services") as described in Article I and Exhibit "A"; and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in Massachusetts the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et seq.; and

WHEREAS, the documents and data transferred from Massachusetts LEAs and created by the Provider’s Services are also subject to several Massachusetts student privacy laws, including Massachusetts student record regulations, 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to Exhibit “A”, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest. Provider shall be under the direct control and supervision of the LEA for use of Pupil Records solely to perform the cloud security and related Services and as instructed by LEA.

1. Nature of Services Provided. The Provider has agreed to provide the cloud security and related Services described in Exhibit “A”.
3. **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit “A”, LEA may provide the categories of data described in the Schedule of Data, attached hereto as Exhibit “B”.

4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

**ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated by this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the LEA maintains that Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The Provider will cooperate and provide Student Data (to the extent Provider has any such Student Data) within ten (10) days at the LEA’s written request to support@cloudlock.com and privacy@cisco.com.

2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information on the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of Services. Provider shall reasonably cooperate and respond within ten (10) days to the LEA’s written request for Personally Identifiable Information in a pupil’s records held by the Provider (if applicable) to view or correct as necessary provided such written request is delivered to support@cloudlock.com and privacy@cisco.com. To the extent permitted by law, in the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** Omitted.

4. **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall, to the extent permitted by law, redirect the Third Party to request the data directly
from the LEA and shall reasonably cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. Except for Subprocessors in Article II, Section 6, the Provider will not use, disclose, compile, transfer, or sell the Student Data and/or any portion thereof to any other third party or authorize any such third parties to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.

6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

**ARTICLE III: DUTIES OF LEA**

1. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H, and the other privacy statutes quoted in this DPA to the extent they are applicable to the Provider. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as “School Officials.”

2. **Reasonable Precautions.** LEA shall take reasonable precautions designed to secure usernames, passwords, and any other authorized means of gaining access to the Services and hosted data.

3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access or imminent threats thereof from the following email: ssmith@cpsd.us. LEA will reasonably assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

**ARTICLE IV: DUTIES OF PROVIDER**

1. **Privacy Compliance.** The Provider shall comply with all Massachusetts and Federal applicable laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, 603 C.M.R. 23.00 and Massachusetts General Law, Chapter 71, Sections 34D to 34H.

2. **Authorized Use.** Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as
authorized under the statutes referred to in subsection (1), above. Provider also acknowledges
and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof,
including without limitation, any student data, meta data, user content or other non-public
information and/or personally identifiable information contained in the Student Data, without the
express written consent of the LEA, unless it fits into the de-identified information exception in
Article IV, Section 4, there is a court order or lawfully issued subpoena for the information, or
such re-disclosure is to a Subprocessor as outlined in Article II, Section 6 for the purpose of
performing the Services described in Exhibit A.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to
Student Data to comply with all applicable provisions of this DPA with respect to the data shared
under this DPA. Provider agrees to require and maintain an appropriate confidentiality
agreement from each employee or agent with access to Student Data pursuant to the DPA
according to the Provider’s Record Retention Policies.

4. **No Disclosure.** De-identified information, as defined in Exhibit “C”, may be used by the
Provider for the purposes of development, research, and improvement of educational sites,
services, or applications, as any other member of the public or party would be able to use de-
identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-
identified Student Data and not to transfer de-identified Student Data to any party unless (a) that
party agrees in writing not to attempt re-identification, and (b) prior written notice has been
given to the LEA who has provided prior written consent for such transfer. Provider shall not
copy, reproduce or transmit any Student Data obtained under this DPA and/or any portion
thereof, except as necessary to fulfill the Services. Prior to publishing any document that names
the LEA explicitly or indirectly, the Provider shall obtain the LEA’s written approval of the
manner in which de-identified data is presented.

5. **Disposition of Data.** Upon a written request of the LEA or upon termination of the DPA,
Provider shall dispose or delete all personally identifiable data obtained under the DPA and
transfer said data to LEA or LEA’s designee within 45 days of receipt of such written request
according to a schedule and procedure as the Parties may reasonably agree. Nothing in the DPA
authorizes Provider to maintain personally identifiable data obtained under any other writing
beyond the time period reasonably needed to complete the disposition. Disposition may include
(1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise
modifying the personal information in those records to make it unreadable or indecipherable.
Upon LEA’s written request, Provider shall provide written notification to LEA when the Data
has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-
de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The
LEA may employ a “Request for Return or Deletion of Student Data” FORM, a Copy of which
is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will
make commercially reasonable efforts to provide the LEA with any specified portion of the
Student Data within ten (10) days of receipt of said request.
6. **Advertising Prohibition.** Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA.

**ARTICLE V: DATA PROVISIONS**

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data. Provider shall only provide access to Student Data to employees or contractors that are performing the Services, based on the principles of least privilege and “need to know.” Employees with access to Student Data shall have signed confidentiality agreements. All employees with access to Student Records shall have undergone criminal background checks.

   b. **Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA upon LEA’s written request, according to a schedule and procedure as the parties may reasonable agree in Article IV, Section 5. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

   c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the DPA in a protected computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

   d. **Employee Training.** The Provider shall provide periodic security training or awareness to those of its employees who operate or have access to the system. Further, upon LEA’s written request, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

   e. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer (“SSL”), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication or data encryption. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.
f. **Security Coordinator.** Upon LEA’s written request, Provider shall provide the name and contact information of Provider’s Security Coordinator responsible for coordinating and monitoring the security requirements and procedures.

g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall have the right in its agreements with Subprocessors to periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article and shall exercise the right when the Provider reasonably suspects non-compliance.

h. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate or mitigate any identified security and privacy vulnerabilities as soon as may be practicable given the circumstances.

i. **Backups.** Provider agrees to design redundant storage and procedures for recovering Student Data in a manner sufficient to reconstruct it in its original state as found on the last recorded backup provided by LEA in case of Provider’s system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

j. **Audits.** The LEA and/or its duly authorized representatives shall have the right, at LEA’s expense, to audit the security and privacy measures that the Provider has in place to ensure protection of the Student Record or any portion thereof. Such audit shall be conducted with reasonable advanced notice to the Provider, and shall take place during normal business hours to reasonably limit disruption to the Provider’s business. The parties shall mutually and reasonably agree on the time, duration, place, manner, and scope of such audit, which shall occur not more than once per year unless there is a verified breach. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider’s records pertaining to the Provider, LEA and delivery of Services to the Provider.

k. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall promptly (within 48 hours) provide notification to LEA at the following email address: ssmith@cpsd.us after confirmation the incident. Provider shall follow the following process:

a. The security breach notification shall be written in plain language.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

   i. The name and contact information of the reporting LEA subject to this section.

   ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

   iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date
of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. Upon a written request, the Provider will also include any of the following:

i. Information about what the Provider has done to protect individuals whose information has been breached.

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

iii. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine or provide at the time the notice is provided.

d. Provider agrees to adhere to all applicable requirements in the Massachusetts Data Breach law and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary description of said written incident response plan.

f. At the request and with the assistance of the District, to the extent it is mandated by the relevant supervisory authority, the Provider shall assist the LEA in notifying the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include, to the extent available to the Provider, the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.

2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

The LEA may terminate this DPA and any service agreement or contract with the Provider if the
Provider breaches any material terms of this DPA and fails to cure such breach within thirty (30) business days after receiving written notice requiring such breach to be cured.

3. **Effect of Termination Survival.** If the DPA is terminated, upon LEA’s written request, the Provider shall destroy all of LEA’s Student data pursuant to Article V, section 1(b).

4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to comply with the applicable privacy protections, including those found in FERPA, IDEA, COPPA, PPRA, 603 CMR 28.00, 603 C.M.R. 23.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives below.

The designated representative for the Provider for this Agreement is:

<table>
<thead>
<tr>
<th>Name</th>
<th>Thomas Fitzgerald</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Director Legal</td>
</tr>
<tr>
<td>Address</td>
<td>8135 Maple Lawn Blvd., FULTON, MARYLAND 20759, UNITED STATES</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>+1 443 430 7025</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:tofitzge@cisco.com">tofitzge@cisco.com</a></td>
</tr>
</tbody>
</table>

The designated representative for the LEA for this Agreement is:

<table>
<thead>
<tr>
<th>Name</th>
<th>Steve Smith</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Information, Communications, and Technology Services Cambridge Public Schools Cambridge, MA 02138</td>
<td></td>
</tr>
</tbody>
</table>

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties.
Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF MASSACHUSETTS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF MIDDLESEX COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.

10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **Electronic Signature:** The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with Massachusetts and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it
is not in its original form or is not an original.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

12. Multiple Counterparts: This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

ARTICLE VII - GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit “F”), be bound by the terms of this to any other school district who signs the acceptance in said Exhibit.

[Signature Page Follows]
IN WITNESS WHEREOF, the parties have executed this Massachusetts Student Data Privacy Agreement as of the last day noted below.

CAMBRIDGE PUBLIC SCHOOLS

[Signature]

Date: 7/11/19

Printed Name: Kenneth N. Salim, Ed.D. Title: Superintendent of Schools

CISCO SYSTEMS, INC.

[Signature]

Date: December 12, 2018

Printed Name: [Authorized Signatory] Title: [Title]

APPROVED BY LEGAL

EXHIBIT "A"
DESCRIPTION OF SERVICES

a. CloudLock, CASB and Cybersecurity-as-a-Service provider, protecting enterprises from compromised accounts, cloud malware, and data breaches in the cloud.
EXHIBIT “B”
SCHEDULE OF DATA
For categories of data collected, processed and/or stored by the Cisco Cloudlock cloud service, see the Cisco Cloudlock Privacy Data Sheet at https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html
EXHIBIT “C”

DEFINITIONS

Affiliate: means any entity that directly or indirectly controls, is controlled by, or is under common control with, another entity, for so long as such control exists. In the case of companies and corporations, "control" and "controlled" mean beneficial ownership of more than fifty percent (50%) of the voting stock, shares, interest or equity in an entity. In the case of any other legal entity, "control" and "controlled" mean the ability to directly or indirectly control the management and/or business of the legal entity.

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

First Name
Last Name
Telephone Number
Discipline Records
Special Education Data
Grades
Criminal Records
Health Records
Biometric Information
Socioeconomic Information
Political Affiliations
Text Messages
Student Identifiers
Photos
Videos
Grade

Home Address
Subject
Email Address
Test Results
Juvenile Dependency Records
Evaluations
Medical Records
Social Security Number
Disabilities
Food Purchases
Religious Information
Documents
Search Activity
Voice Recordings
Date of Birth
Classes

General Categories:
Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student’s Educational Record

Information in the Student’s Email

Provider: For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or student’s parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information.

Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Massachusetts and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider’s General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.
Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Third Party: The term “Third Party” means an entity that is not the provider or LEA.

EXHIBIT “D”

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

   Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

   [Insert categories of data here]

   Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

   Disposition shall be by destruction or deletion of data.

   Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

   [Insert or attach special instructions.]

3. Timing of Disposition

   Data shall be disposed of by the following date:

   As soon as commercially practicable

   By (Insert Date)

4. Signature

   (Authorized Representative of LEA

   ____________________________

   Date

1104586v1
5. Verification of Disposition of Data

Authorized Representative of Company

Date

OPTIONAL EXHIBIT “E”

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and the LEA to any other school district (“Subscribing LEA”) who accepts this General Offer through its signature below. The Provider agrees that the information on the next page will be replaced throughout the Agreement with the information specific to the Subscribing LEA filled on the next page for the Subscribing LEA. This General Offer shall extend only to privacy protections and Provider’s signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provide by LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in the Original Service Agreement; or three (3) years after the date of Provider’s signature to this Form. Provider shall notify the LEA in the event of any withdrawal so that this information may be transmitted to the Subscribing LEAs.

CISCO SYSTEMS, INC.

BY: ____________________________ Date: ____________________________
Printed Name: ____________________________ Title/Position: ____________________________

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA’s individual information is contained on the next page. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: ____________________________ Date: ____________________________
Printed Name: ____________________________ Title/Position: ____________________________
SCHOOL DISTRICT NAME: ____________________________
DATE: ____________________________
DESIGNATED REPRESENTATIVE OF LEA:
<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
</tbody>
</table>

COUNTY OF LEA: ___________________________