



## Data Sharing/Use Agreement

Between

Jefferson County Board of Education

And

*Pear Deck, Inc.*

This Data Sharing/Use Agreement ("Agreement") between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools ("JCPS"), and *Pear Deck, Inc.*, a corporation organized under the laws of Delaware. ("Services Provider" or "Pear Deck") describes the services and products to be provided to JCPS by Services Provider under the terms of Pear Deck's Terms of Service, as may be amended from time to time a current version of which is located at [www.peardeck.com/terms-of-service](http://www.peardeck.com/terms-of-service) ("Service Agreement") (together, the "Agreement"), and the means to be used by Services Provider to ensure the confidentiality and security of information and data exchanged between JCPS and Services Provider in connection with the provision of the services. To the extent of any conflict between the Data Sharing Agreement and the Service Agreement, the terms of this Data Sharing Agreement shall control. To the extent of any conflict between the Service Agreement and the contract referenced in paragraph B.1. below, the terms of the contract referenced in paragraph B.1. shall control. "Pear Deck Parties" means Pear Deck, its affiliates, licensors, and suppliers, and their respective officers, directors, employees, shareholders, agents and representatives.

### A. PERIOD OF THE DATA SHARING AGREEMENT

This Agreement shall be effective as of July 28, 2021 and will terminate when the services contract referenced in Paragraph B.1. below terminates, unless terminated earlier by either party pursuant to Section H or the Service Agreement.

### B. SCOPE OF THE AGREEMENT AND INTENDED USE OF THE DATA

1. Services Provider will provide the following Pear Deck services to JCPS under the terms of a services contract between JCPS and Services Provider effective July 28, 2021: Pear Deck is a web-based software application for student engagement (the "Pear Deck Offerings"). Teachers build lessons on Pear Deck in order to further classroom equity, student engagement, formative assessment and data-driven instruction.
2. JCPS and Services Provider agree that Services Provider is an organization to which JCPS can disclose, personally identifiable information from an education record of a student, as defined in 34 CFR 99.3, under the "school official exception" of the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g)

and 34 C.F.R. 99.31 (a)(1) ("FERPA"), because the disclosure is to a contractor to whom JCPS has outsourced institutional services or functions for which JCPS would otherwise use employees; the contractor is under the direct control of JCPS with respect to the use and maintenance of education records; and the contractor is subject to the requirements of 34 CFR 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

3. JCPS shall disclose to Services Provider, confidential, personally identifiable information from an education record of a student, as defined in 34 C.F.R. 99.3, under the "school official exception" of FERPA, 34 C.F.R. 99.31 (a)(1), when the disclosure is within such exception as stated in Paragraph B.2 above and Services Provider has a legitimate educational interest for access to such education records. The Student Data is described in a document attached to this agreement as **Attachment A**. Services Provider shall use personally identifiable information from education records in order to perform, improve, and support the Pear Deck Offerings. Services Provider shall notify JCPS of any changes to the list of disclosed data necessary for the Pear Deck Offerings or any changes to the scope, purpose or duration of the services themselves through sending JCPS's Stefanie Mills notice of updates with such notice of updates being able to be made through sending JCPS's Stefanie Mills notice of updates to Services Providers' Product Policy and/or Terms via email at [stefanie.mills@jefferson.kyschools.us](mailto:stefanie.mills@jefferson.kyschools.us). Any agreed upon changes to the data disclosed shall be reduced to writing and included in an update to Attachment A to this Agreement. Any agreed upon changes to the scope, purpose or duration of the services shall be reduced to writing and included in an amendment to the services contract described in Paragraph B.1 above.
4. Services Provider and JCPS shall work cooperatively to determine the proper medium and method for the transfer of Student Data between each other.

### **C. CONSTRAINTS ON USE OF DATA**

Regarding Student Data:

1. Services Provider agrees that the Pear Deck Offerings shall be provided in a manner that does not reasonably permit personal identification of parents and students by individuals other than JCPS (including JCPS Authorized Users), representatives of Services Provider that have legitimate educational interests in the information, or as otherwise required by law or permitted by this Agreement, including but not limited to, in response to a subpoena or court order. In the event of a subpoena or a court order, Services Provider shall notify JCPS prior to production to the extent legally permissible in order to allow JCPS to meet its notification obligations under FERPA.
2. Services Provider will not contact the individuals included in the data sets without obtaining advance written authorization from JCPS, unless: (1) to respond to a direct inquiry from such student to Pear Deck (in which case, Pear Deck shall use reasonable efforts when reasonably practicable to inform such student to

contact JCPS with his/her inquiry); (2) to obtain consent from eligible students; (3) in connection with a health or safety emergency; or (4) such contact is required by law, pursuant to a subpoena, or court order. Prior to any production or disclosure, Services Provider shall notify JCPS to the extent legally permissible in order to allow JCPS to meet its notification obligations under FERPA.

3. Services Provider shall not re-disclose any Student Data to any other requesting individuals, agencies, or organizations without prior written authorization by JCPS, unless required by law or court order. Prior to any production or disclosure, Services Provider shall notify JCPS to the extent legally permissible in order to allow JCPS to meet its notification obligations under FERPA.
4. Services Provider shall use the Student Data only to fulfill the purposes of the Service Agreement. The data shall not be used for personal gain or profit

#### **D. DATA CONFIDENTIALITY AND DATA SECURITY**

Services Provider agrees to the following confidentiality and data security statements:

1. Services Provider acknowledges that the Student Data is confidential data and proprietary to JCPS, and agrees to protect the data from unauthorized disclosures and to comply with all applicable Local, State and Federal confidentiality laws and regulations including but not limited to, as applicable, FERPA; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; 7 C.F.R. 245.6 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.
2. If the performance of this Agreement involves the transfer by JCPS to Services Provider of any personally identifiable information from education records (as defined in FERPA), Services Provider agrees to:
  - a. In all respects comply with the provisions of FERPA.
  - b. Use any such data for no purpose other than to fulfill the purposes of the Services Agreement described in Paragraph B.1 above, and not share any such data with any person or entity other than Services Provider and its employees, contractors and agents, or permitted assignees (see Section P) without the prior written approval of JCPS.
  - c. Require all employees, contractors and agents of Services Provider to comply with all applicable provisions of FERPA with respect to any such data.
  - d. Maintain any such data in a secure computer environment, and not copy, reproduce or transmit any such data except as necessary to fulfill the purposes of the Services Agreement described in Paragraph B.1 above.
  - e. Provide the Pear Deck Offerings under the Services Agreement above in a

manner that does not permit the identification of an individual student by anyone other than employees, contractors or agents of Services Provider having a legitimate interest in knowing such personal identification.

- f. Destroy or return to JCPS any such data obtained under this Agreement at the written instruction of JCPS in accordance with FERPA.
3. Services Provider shall not release or otherwise reveal, directly or indirectly, Student Data to any individual, agency, entity, or third party not permitted by this Agreement, unless such disclosure is required by law, subpoena, or court order. If Services Provider becomes legally compelled to disclose any Student Data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then Services Provider shall use all reasonable efforts to provide JCPS with prior notice before disclosure to the extent legally permissible so that JCPS may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure JCPS's compliance with the confidentiality requirements of federal or state law; provided, however, that Services Provider will use all reasonable efforts to maintain the confidentiality of Student Data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, Services Provider will only disclose that portion of Student Data that Services Provider is legally required to disclose.
4. Services Provider shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the Student Data.
5. Services Provider shall not use data shared under this Agreement for any purpose other than the Service Agreement described in Paragraph B.1 above. Nothing in this Agreement shall be construed to authorize Services Provider to have access to additional data from JCPS that is not included in the scope of this Agreement (or addenda). Services Provider understands that this Agreement does not convey ownership of the Student Data to Services Provider.
6. Services Provider shall take reasonable security precautions and protections to ensure that persons not authorized to view the Student Data do not gain access to such data. Reasonable security precautions and protections include, but are not limited to:
  - a. Creating, distributing, and implementing data governance policies and procedures which protect data through appropriate administrative, technical and physical security safeguards, and outline staff responsibilities for maintaining data security;
  - b. Encrypting all Student Data carried on mobile computers/devices;
  - c. Encrypting Student Data before it is transmitted electronically;
  - d. Requiring that users be uniquely identified and authenticated before

- accessing Student Data;
- e. Establishing and enforcing well-defined data privilege rights which restrict users' access to Student Data necessary for this to perform their job functions;
  - f. Ensuring that all staff accessing data sign either a sensitive data handling policy (as updated from time to time) or a nondisclosure statement, both attached as **Attachment B**, and maintain copies of signed statements;
  - g. Securing access to any physical areas/electronic devices where Student Data are stored;
  - h. Installing a firewall to permit or deny network transmissions based upon a set of rules; and
  - i. Installing anti-virus software to protect the network.
7. If Services Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act"), Services Provider shall secure, protect and maintain the confidentiality of the Personal Information (as defined below) by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:
- a. "Personal Information" is defined in accordance with KRS 61.931(6) as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one or more of the following data elements:
    - i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
    - ii. A Social Security number;
    - iii. A taxpayer identification number that incorporates a Social Security number;
    - iv. A driver's license number, state identification card number or other individual identification number issued by an agency;
    - v. A passport number or other identification number issued by the United States government; or
    - vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and

Accountability Act), except for education records covered by FERPA.

- b. As provided in KRS 61.931(5), a "non-affiliated third party" means "any person that has a contract or agreement with an agency as defined by KRS 61.931(1) and receives (accesses, collects or maintains) personal information from the agency pursuant to the contract or agreement."
  - c. Services Provider shall not re-disclose, without the written consent of JCPS or otherwise as required by law or permitted by the Agreement, any "personal information," as defined in KRS 61.931, of a student or other persons, such as employees.
  - d. Services Provider agrees to reasonably cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.
  - e. Services Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.
8. If Services Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Services Provider agrees that:
- a. Services Provider shall not process Student Data for any purpose other than providing, improving, developing, or maintaining the integrity of its Pear Deck Offerings, unless the provider receives express permission from the eligible student or student's parent. If Services Provider seeks express permission from eligible student or student's parent, Services Provider shall work with the student's school and JCPS to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."
  - b. Pursuant to KRS 365.734(2), Services Provider shall not in any case process Student Data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.
  - c. Pursuant to KRS 365.734(2), Services Provider shall not sell, disclose, or otherwise process Student Data for any commercial purpose.
  - d. Services Provider certifies that it will comply with KRS 365.734(2).
9. Services Provider shall report all known or reasonably suspected unauthorized disclosure of the Student Data, in any format, to Dr. Kermit Belcher, Chief Information Officer. The report shall include, to the extent known (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discovered the incident; (3) the date and time the incident was discovered; (4) the nature of the incident (e.g. system level electronic breach, an electronic breach of one computer or device, or a breach of hard copies of records, etc.); (5) a description of the information lost or compromised; (6) the name of



the electronic system and possible interconnectivity with other systems; (7) the storage medium from which information was lost or compromised; (8) the controls in place to prevent unauthorized use of the lost or compromised information; (9) the number of individuals potentially affected; and (10) whether law enforcement was contacted.

10. Services Provider shall use commercially reasonable efforts to securely and permanently destroy the Student Data, and any and all hard and soft (electronic) copies thereof, upon the termination of this Agreement. Services Provider agrees to require all employees, contactors, or agents of any kind using JCPS Student Data to comply with this provision. Services Provider agrees to document the methods used to destroy the data, and upon request, provide certification to JCPS that the Student Data has been destroyed.
11. For purpose of this Agreement and ensuring Services Provider's compliance with the terms of this Agreement and all application of the state and Federal laws, Services Provider designates **Zahir Zubair, Director PMO & IT** (or an alternative designee specified in writing) as the temporary custodian ("Temporary Custodian") of the data that JCPS shares with Services Provider. JCPS will release all data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the return or destruction of the data as described below. JCPS or its agents may, upon request, review the records Services Provider is required to keep under this Agreement.
12. Services Provider acknowledges that any violation of this Agreement and/or the provisions of FERPA or accompanying regulations related to the nondisclosure of protected student information constitutes just cause for JCPS to immediately terminate this Agreement.
13. Services Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of \$5M. Upon request, Services Provider shall furnish the certificate of insurance evidencing this coverage. The certificate of insurance shall name the Board of Education of Jefferson County as additional insured in the Description of Operations section of the Certificate of Insurance which shall read:

Board of Education of Jefferson County  
Attn: Insurance/Real Estate Dept.  
3332burg Road  
Louisville, Kentucky 40218
14. Services provider shall maintain, during the term of this Agreement, ISO27001 or SOC2 certification.. If Services Provider is unable to provide ISO27001 or SOC2 certification, minimum requirements on a JCPS-provided standardized questionnaire must be met. If Services Provider is unable to reasonably meet the requirements of the JCPS-provided standardized questionnaire within a commercially reasonable amount of time after Service

Provider has received written notice from JCPS of any remediation or changes, either party may terminate the Agreement without default upon written notice. Upon request, Services Provider shall furnish a current ISO27001, SOC2 certification, or updated questionnaire.

**E. FINANCIAL COSTS OF DATA-SHARING**

Any costs associated with data sharing and payments to Services Provider will be made under services contract described in Paragraph B.1 above.

**F. OBLIGATIONS OF JCPS**

During the term of this Agreement, JCPS shall:

1. Prepare and deliver the data described in **Attachment A**.

**G. LIABILITY AND INDEMNIFICATION**

**1. Limitation of Liability. TO THE EXTENT PERMITTED BY LAW, NEITHER PARTY (INCLUDING PEAR DECK PARTIES) WILL BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF THIS AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.**

EXCEPT FOR UNAUTHORIZED DISCLOSURES OF STUDENT DATA IN VIOLATION OF FERPA AND/OR KRS § 365.734, IN NO EVENT WILL SERVICES PROVIDER'S (INCLUDING PEAR DECK PARTIES') TOTAL LIABILITY HEREUNDER EXCEED TWICE THE AMOUNT THAT JCPS PAID SERVICES PROVIDER FOR THE PEAR DECK OFFERING(S) GIVING RISE TO SUCH CLAIM IN THE CALENDAR YEAR IN WHICH SUCH CLAIM AROSE. IN THE EVENT OF AN UNAUTHORIZED DISCLOSURE OF STUDENT DATA IN VIOLATION OF FERPA AND/OR KRS § 365.734, IN NO EVENT WILL SERVICES PROVIDER'S (INCLUDING PEAR DECK PARTIES') TOTAL LIABILITY FOR SECURITY BREACHES IN VIOLATION OF FERPA AND/OR KRS § 365.734 HERUNDER EXCEED TWICE THE AMOUNT THAT JCPS PAID SERVICES PROVIDER FOR THE PEAR DECK OFFERING(S) GIVING RISE TO SUCH CLAIM IN THE CALENDAR YEAR IN WHICH SUCH CLAIM AROSE.



**2. Indemnification.** Services Provider shall indemnify and hold harmless JCPS from and against all claims, costs, damages, or expenses (including reasonable attorneys' fees) ("Claims") against JCPS up to and not to exceed, in aggregate, twice what JCPS paid Services Provider for the Pear Deck Offering(s) giving rise to such claim, for any third party Claim to the extent such Claim is caused by Services Providers' unauthorized disclosures of Student Data in violation of FERPA and/or KRS § 365.734. The foregoing obligations are conditioned on JCPS providing Services Provider reasonable notice of such action, notifying Services Provider promptly in writing of such action, JCPS giving Services Provider sole control of the defense thereof and any related settlement negotiations, and JCPS cooperating and, at Services Provider's reasonable request and expense, assisting in such defense.

#### **H. TERMINATION**

1. This Agreement may be terminated as follows, after notification via the United States Postal Service (certified mail or registered mail) or recognized overnight delivery service (e.g., UPS, DHL, or FedEx):
  - a. By either party in the event of a material breach of this Agreement by another party provided however, the breaching party shall have thirty (30) days to cure such breach and this Agreement shall remain in force.
  - b. By either party after thirty (30) days advance written notice to the other party, for any reason or no reason.
2. The confidentiality provisions of this Agreement shall survive the termination of this Agreement until Student Data is no longer maintained by Services Provider. If this Agreement is terminated by either party for material breach or for any other reason with thirty (30) days written notice, within thirty (30) days of the termination the confidential information shall be returned or destroyed within thirty (30) days of the termination and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11. If this Agreement terminates at the end of the term described in Section A, within seven (7) days after the end of the term, Services Provider shall return or destroy all Student Data and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11.
3. Destruction of the Student Data shall be accomplished by utilizing commercially reasonable methods of confidential destruction, including but not limited to shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.

#### **I. MODIFICATION**

No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.

**J. QUALITY OF SERVICES**

JCPS reserves the right to review Services Provider's performance under this Agreement for effectiveness in serving the specific purposes as outlined in Paragraph B.1. Failure of Services Provider to perform in a manner that meets or exceeds the quality standards for JCPS shall serve as grounds for termination of this Agreement, subject to Service Provider's right to cure under Section H.1.a. of this Agreement.

**K. BREACH OF DATA CONFIDENTIALITY**

Services Provider acknowledges that the breach of the Data Sharing Agreement may result in irreparable and continuing damage to JCPS for which money damages may not provide adequate relief. In the event of a breach or threatened breach of this agreement by Services Provider, JCPS, in addition to any other rights and remedies available to JCPS at law or in equity, may be entitled to preliminary and permanent injunctions to enjoin and restrain the breach or threatened breach. If the United States Department of Education's Family Policy Compliance Office determines that Services Provider has violated paragraph 34 C.F.R. 99.31(a)(6)(iii)(B), JCPS may not allow Services Provider access to personally identifiable information from its education records for at least five (5) years.

**L. CHOICE OF LAW AND FORUM**

The Data Sharing Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Kentucky. Any action or Claim arising from, under or pursuant to this Data Sharing Agreement shall be brought in the state and federal courts of Jefferson County, Kentucky, and the parties expressly waive the right to bring any legal action or Claims in any other courts.

**M. WAIVER**

No delay or omission by either party in exercising any right under this Agreement shall operate as a waiver of that or any other right or prevent a similar subsequent act from constituting a violation of this Agreement.

**N. SEVERABILITY**

If any part of this Data Sharing Agreement is held to be void, against public policy or illegal, the balance remaining provisions of this Data Sharing Agreement shall continue to be valid and binding.

**O. NOTICES**

Any notices or reports by one party to the other party under this Data Sharing Agreement shall be made in writing, to the address shown in the signature portions of this Data Sharing Agreement, or to such other address as may be designated in writing by one party to the other. Notices shall be effective when received if personally delivered or by overnight carrier by a well-recognized carrier, or three days after mailing via United States mail if mailed.

**P. RELATIONSHIP OF PARTIES**

JCPS is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor JCPS shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.


**Q. ENTIRE AGREEMENT; ASSIGNMENT**

1. This Agreement, together with any attachments hereto and any amendment or modifications that may hereafter be agreed to, constitute the entire understanding between the parties with respect to the subject-matter hereof and supersede any and all prior understandings and agreements, oral and written, relating hereto. Sections G(1), K-P shall survive termination of this Data Sharing Agreement.

2. Services Provider shall not assign this Data Sharing Agreement or any portion thereof to third party without the prior written consent of JCPS, except in connection with a merger, acquisition, or sale of all or substantially all of Services Provider's assets provided that the successor entity is bound by this same Data Sharing Agreement, and any other unpermitted attempted assignment without such prior written consent in violation of this Section Q shall automatically terminate this Data Sharing Agreement.

**AGREED:**

Pear Deck, Inc.  
2030 E Maple Ave., Suite 100  
El Segundo, CA 90245

BY:    
6CD8C493E787445...

Name: Michael Jonas

Title: Chief Financial Officer

Date: 7/14/2021

**AGREED:**

Jefferson County Board of Education  
3332 Newburg Road  
Louisville KY 40218

BY: \_\_\_\_\_

Name: Martin A. Pollio, Ed. D.,

Title: Superintendent

Date: \_\_\_\_\_

## **CONFIDENTIAL INFORMATION TO BE DISCLOSED**

- **Student's School-Managed Account Information and Association Information:** For students who log into Pear Deck with a School-Managed Account, we collect student's name, email address, the school-managed account ID ( for example the Google ID or Microsoft ID), as well as identifiers and associated information necessary to associate a student with a certain device, account, presentation, teacher, and/or school. When a student joins a session with a code, we do not collect student name or email address to join such session.
- **Activity Information:** We collect additional information about the student's activity within a presentation, including engagement with and any student content generated in the session. This may include, free text, multiple choice answers, drawings, or URLs.
- **Device and Usage Information:** We collect general device and usage information such as IP address, device identifier, operating system, browser type, non-precise geographic location (e.g. zip code and city), technical information about your device, system and app software, and peripherals, and date and time stamps associated with login.

## **Attachment B**

### **SERVICE PROVIDER'S EMPLOYEE NONDISCLOSURE STATEMENT**

**Pear Deck has merged as a subsidiary with another company called GoGuardian. We have attached a copy of GoGuardian's Sensitive Information Handling Policy for your information. Sensitive Information Handling Policy**

In the course of offering its products and services to customers, GoGuardian accesses and collects certain information about its customers, which are typically K-12 schools and districts as well as their students, teachers, staff, administrators, and potentially parents/guardians depending on GoGuardian's current product offerings. Some of this information is sensitive and legally protected as specified in more detail by GoGuardian's Privacy Team and what we will label as "*Sensitive Information*."

Sensitive Information includes "any data that alone or in combination, including in combination with publicly-available data, could reasonably be used to identify a current or former K-12 student, including contact information, academic records, self-harm or medical-related data, extra-curricular activities, class information, and other similar information. Please note that Sensitive Information includes "*Personal Student Information*" as defined in the GoGuardian Privacy Policy available at <https://www.goguardian.com/privacy.html>. When in doubt, you should assume that any information directly or indirectly relating to students, should be treated as Sensitive Information.

**GoGuardian takes the privacy of users' and students' data seriously, and therefore sets forth the following policy for you concerning proper treatment of Sensitive Information:**

Collection and Storage of Sensitive Information. GoGuardian centralizes its storage of Sensitive Information on its servers hosted by approved third parties. You may not to print, save, copy, or locally store Sensitive Information, except temporarily in a secure manner and only to the extent necessary to perform your job functions, and you must immediately destroy or delete any such temporary copies upon conclusion of the activity giving rise to the necessity of saving, copying, or storing of the Sensitive Information.

Access and Use of Sensitive Information. GoGuardian is generally limited to accessing and using Sensitive Information only when necessary to support, provide, and improve our product offerings to schools. Accordingly, you may only access and/or use Sensitive Information as necessary to perform your job duties and functions for GoGuardian.

Use of Data - No Targeted Advertisements or Amassing of Student Profiles. There are important legal restrictions on the use of Sensitive Information, which often vary from state-to-state through state student privacy laws and from customer-to-customer through contractual agreements (e.g., data privacy addenda). You will not use Sensitive Information to market to anyone or behaviorally-target advertisements. You may not use Sensitive Information to amass student profiles, except in furtherance of K-12 legitimate educational purposes and in compliance with applicable law. When in doubt, please consult the Privacy Team about your desired data use.

Confidentiality and Protection of Sensitive Information. You may not disclose Sensitive Information to individuals or organizations outside of GoGuardian, other than to GoGuardian-approved, contractual third parties under confidentiality obligations that need such information to perform services on GoGuardian's behalf. If you are granted access to Sensitive Information, you may only discuss that information with other GoGuardian employees that have a need to know such Sensitive Information and have been granted by GoGuardian the same or greater access levels to Sensitive Information. Further, you must use

applicable, industry standard administrative, technical, legal, and administrative safeguards to protect Sensitive Information in compliance with GoGuardian's then-current security and data protection policies and procedures, which will be provided to you as applicable.

Unauthorized Use and Disclosure of Sensitive Information. Out of respect to our customers and their students as well as to abide by our legal requirements and contractual requirements with customers (e.g., data privacy addendum), potential and actual unauthorized uses and disclosures (e.g., including security breaches) of Sensitive Information must be escalated and prioritized immediately. Accordingly, you agree to immediately notify GoGuardian's Chief Technology Officer and Privacy Team upon learning of a potential or actual misuse or unauthorized disclosure of Sensitive Information to allow GoGuardian to timely investigate and address such concerns. You also agree to follow the then-current action response and/or breach response protocols to help resolve the misuse or disclosure issue.

De-identifying Data. GoGuardian has certain obligations to de-identify Sensitive Information before retaining, using, sharing, or disclosing any data derived from Sensitive Information. These responsibilities to de-identify Sensitive Information result from a variety of sources, including customer requests during the course of their license with GoGuardian, parent/guardian/eligible student requests, obligations that arise upon termination/completion of a customer's license with GoGuardian, GoGuardian's Privacy Policy, and/or applicable law.

Depending on a particular customer contract, applicable law, and desired use of such data (e.g., K-12 research vs. publishing a data set), you may be restricted in which type of data you may utilize and how the data must be de-identified before engaging in a particular use or sharing or disclosure (e.g., publishing) of such data. Accordingly, you agree to properly de-identify data to the standard necessary to protect the data from the risk of re-identification and to comply with any restrictions regarding such data use in accordance with the Privacy Team's then-current guidelines, policies, and procedures, as applicable, and to consult the Privacy Team if you have any questions about your particular situation.

Prohibition on Re-Identifying Data. Once Sensitive Information has been de-identified, you agree not to attempt to re-identify the data to determine the individuals who were associated with such data. Additionally, you agree to take appropriate, industry standard precautions and consult the Privacy Team and technical teams to ensure that others to whom you share or disclose (e.g., publish data) de-identified data are unable to re-identify individuals, even taking into account all publicly-available information (e.g., census data, school website data, and online news).

Lastly, you agree to follow the then-current guidelines, policies, and procedures (including GoGuardian's Privacy Policy currently available at) regarding the treatment of Sensitive Information beyond the foundational guidelines that are set forth in this policy. The Privacy Team is available to answer any questions about this policy, treatment of Sensitive Information, and the application of this policy to your specific initiatives at GoGuardian.

Because the privacy of our users is of the utmost important to GoGuardian and critical to its users and their students, failure to follow this policy may lead to disciplinary action and/or termination from GoGuardian.