

APPENDIX A

STUDENT LEVEL DATA PROTECTION

The services or functions included in the Cloud Services Agreement between CareDox and Park City School District (“Parties”) involve CareDox obtaining or using education records or other personally identifiable information. Park City School District (“PCSD”) is subject to Family Educational Rights and Privacy Act (“FERPA”) 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. Part 99, which generally requires written consent for disclosure of educational record or personally identifiable information to third parties.

Written consent is not required for school officials. FERPA provides that a contractor, consultant, volunteer, or other outside party may be treated as a school official if the contracting party is: (a) providing services or functions that PCSD would otherwise use employees, (b) under the direct control of PCSD with respect to the use and maintenance of education records and personally identifiable information, (c) subject to the requirements of 34 C.F.R. 99.33(a), and (d) limiting access within the contractor’s organization to those who have a legitimate educational interest. 34 C.F.R. 99.31(a)(1)(i)(B).

In addition, the Utah Student Data Protection Act, Utah Code Ann. §§ 53A-1-1401, *et. seq.* requires that third-party contractors using personally identifiable student data adhere to certain requirements regarding the protection of student data.

PCSD and CareDox desire to have CareDox treated as a school official within the FERPA exception in 34 C.F.R. 99.31(a)(1)(i)(B) and to comply with state and federal student and family privacy laws, including the Utah Student Data Protection Act. To protect the privacy of students and parent data, PCSD and CareDox include and incorporate this Appendix to the Cloud Services Agreement (“Contract”).

The Parties agree as follows:

1. The term of this Appendix shall remain in effect through the duration of the Contract. In the event of a conflict between the terms of this Appendix and the terms of the Contract, this Appendix shall control.
2. The following definitions apply to the Appendix:
 - a. “Education records” includes all information accessed, collected, stored, processed, disclosed, de-identified, created, or used by CareDox, including metadata and personally identifiable information, in relation to the Agreement. CareDox acknowledges and agrees that student health records and health information in the possession of PCSD are considered education records under FERPA and this Appendix.
 - b. “Metadata” includes all information created manually or automatically to provide meaning or context to other data.
 - c. “Personally Identifiable Information” or “PII” includes both direct identifiers (such as a student’s or other family member’s name, address, student number, or biometric number) and indirect identifiers (such as a student’s date of birth, place of birth, or mother’s maiden name). Indirect identifiers that constitute PII also

include metadata about student interaction with an app or service, or other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

3. CareDox agrees that all data files, including derivative files, and all data files resulting from merges, matches, or other uses of education records provided or obtained pursuant to the Contract are subject to this Appendix.
4. CareDox's services provided to PCSD are services for which PCSD would otherwise use employees.
5. CareDox is a party acting for PCSD, who has direct control of the use and maintenance of education records. All education records are in the legal and rightful custody and control of PCSD. CareDox acquires no rights or licenses to use the education records for any other purpose than for performing the services set forth in the Contract.
6. CareDox has a legitimate educational interest in the education records based upon the Contract.
7. CareDox shall limit access within its organization to individuals whom CareDox has determined to have legitimate educational interests in the education records.
 - a. CareDox shall require a non-disclosure agreement be signed by those individuals within its organization that CareDox determines will have access to the education records because the individuals have a legitimate educational interest in the education records.
 - b. CareDox shall maintain past and current lists of all individuals to whom it has determined to allow access to education records because the individuals have legitimate educational interest in the education records.
 - c. CareDox shall maintain each non-disclosure agreement signed by its employees at its facility and shall permit inspection of the same by PCSD, upon request.
 - d. CareDox shall maintain an audit trail for the duration of the Contract which reflects the granting and revoking of access privileges for the purposes of tracking any unauthorized use or access to PCSD data. A copy of this audit trail may be requested by PCSD at any time and shall be provided within ten days of PCSD's request.
 - e. CareDox shall further notify PCSD in writing within two business days if an individual's privileges to access education records has been withdrawn for the purposes of tracking any unauthorized use or access to PCSD data and the date withdrawal occurred.
 - f. CareDox shall require and ensure annual training of those individuals determined to have access due to a legitimate educational interest in the education records. The training shall include the federal and state laws relating to student and family privacy and best practices for maintaining student and family privacy.

- g. CareDox shall maintain past and current lists of individuals attending training and the related training materials.
 - h. CareDox shall not disclose the education records to individuals within CareDox who have not been determined to have a legitimate educational interest, who have not received training, and who have not signed a nondisclosure agreement.
 - i. PCSD, or its designee shall have the right to audit CareDox's compliance with this Appendix and CareDox shall provide such access and information as is reasonably necessary in furtherance of same. PCSD shall provide at least 48 hours advance written notice of its intent to conduct an audit.
- 8. CareDox shall only access, collect, store, process, or use the education records, as necessary to provide the services set forth in the Contract for its legitimate educational interest in the education records.
- 9. Data disclosed by PCSD to CareDox includes records that: (1) may directly relate to a student; (2) may contain personally identifiable information, and (3) are maintained by an educational agency or institution or by a party acting for the agency or institution.
- 10. CareDox shall not re-disclose the education records to any other party without the prior consent of the parent or eligible student, unless said party is providing services to PCSD on behalf of CareDox under the terms of the Agreement. For avoidance of doubt, CareDox shall ensure that any third parties with whom CareDox might contract to provide services to PCSD under the Agreement comply with the terms of this Appendix and CareDox shall be solely responsible for ensuring compliance with same. CareDox uses a nationally recognized hosting provider in connection with the Services. PCSD understands that CareDox's agreement with the hosting provider cannot be modified regarding the requirements of this Appendix, nor can CareDox grant any audit or other access rights to the facilities or systems of the host. As such, the provisions of this Appendix shall apply to CareDox's systems and facilities, not those of the host. The host does, however, make available extensive documentation regarding its security practices and measures. Such documentation is readily available to PCSD for review.
- 11. CareDox shall protect all education records in a manner that does not permit disclosure of the educational records to anyone other than those individuals within its organization and third parties providing services to PCSD on behalf of CareDox to whom CareDox has determined to have legitimate educational interests in the education records.
- 12. CareDox shall store and maintain all education records separately from the information of any other records.
- 13. CareDox shall notify PCSD if there are any changes that will materially affect the system where all education records are stored and maintained in a manner that reduces the existing privacy and security protections, and ensure the system is in compliance with industry standards for the security and privacy of education records.
- 14. CareDox shall comply with all Utah state and federal laws relating to student or family privacy and will maintain any and all education records in a manner consistent with such laws, including, but not limited to Utah Code Ann. §§ 53A-1-1410, governing use of student data by third-party contractors. CareDox recognizes that the provisions of

section 53A-1-1410 limit the purposes for which even de-identified data may be used and that these limitations may conflict with other terms of the Contract.

15. CareDox shall notify PCSD in writing immediately upon discovering any breach, or suspected breach of security, or any disclosure of education records to an unauthorized individual within CareDox's organization, or unauthorized re-disclosure to anyone. Notification shall include the date of improper release and a secure transmission of list(s) of affected students or families to assist PCSD in notifying students, parents, or guardians of the improper release as required by federal and state law. CareDox agrees the improper release of any education record constitutes a material breach of the Contract. CareDox shall be liable for any claims or damages that occur from its failure to comply with its obligations in this Appendix.
16. CareDox shall return to PCSD or securely destroy any education records and PII provided pursuant to the Contract upon the earlier of either the expiration or termination of the Contract, unless the parent or legal guardian of a PCSD student provides written authorization to maintain their student's data in their own CareDox account. If CareDox desires to seek such written authorization upon expiration or termination of the Agreement, it shall (a) clearly disclose all relevant terms and conditions and privacy policies applicable to such accounts; and (b) neither express nor imply that PCSD is in any way involved with the ongoing maintenance of such accounts.
17. Notices required by this Appendix shall be provided to:
Andrew Frink, Director of Technology and Chief Privacy Officer at: afrink@pcschoos.us