Data-Sharing & Confidentiality Agreement

COLORADO DEPARTMENT of EDUCATION cde

Purpose: The Colorado Department of Education holds data privacy, confidentiality, and security practices in the highest regard. All data utilized by CDE is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Colorado statute. This document outlines the manner in which CDE staff is to utilize data and protect personally identifiable information. A signed agreement form is required from all CDE staff to verify agreement to adhere to/abide by these practices. The failure to adhere to guidelines may result in personnel action, up to and including termination.

All CDE employees (including contract or temporary) will:

1. Complete CDE cyber-security web training.
2. Complete select FERPA web trainings hosted by the Privacy Technical Assistance Center (PTAC).
3. Obtain appropriate permission from data owners when creating or disseminating reports.
4. Use password-protected state-authorized computers when accessing student/staff level records.
5. NOT share individual passwords for personal computers or data systems with anyone.
6. Log out of any data system/portal and close the browser after each use.
7. Store sensitive data on appropriate-secured location. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive data.
8. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at CDE when disposing of such records.
9. NOT share child/staff-identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, dummy records should be used for such presentations.
10. Redact any personally identifiable information when sharing sample reports with general audiences. Also, take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

    More information: http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011603
11. Delete files containing sensitive data after using them on computers, or move them to secured servers

or personal folders accessible only by authorized parties.

12. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data, the mechanism outlined below in item 13 should be used, or IMS (Information Management Services unit) consulted.
13. Use secure methods when sharing or transmitting sensitive data. The approved method is CDE's Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders is appropriate for CDE internal file transfer.
14. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and Institutional Review Board representative when applicable (i.e. as part of a formal research study) and then only transmit data via approved methods such as described in item ten.
15. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

Colorado Department of Education:
Staff Agreement Concerning Data Sharing & Confidentiality

As an employee of the Colorado Department of Education, I hereby affirm that: (Initial)

_____ I have read the Data Sharing and Confidentiality assurances attached to this agreement form. These assurances address general procedures, data use/sharing, and data security.

Web Trainings

_____ I have watched and completed the Privacy Technical Assistance Center *FERPA 101* and *FERPA 201: Data Sharing* training videos and understand the guidelines set forth. http://ptac.ed.gov/

_____ I have (or will) watch and complete the CDE cyber-security web training and understand the guidelines set forth.

Using CDE Data and Reporting Systems

_____ I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.

_____ I will not share or exchange individual passwords, for either personal computer(s) or CDE system user accounts, with CDE staff or participating program staff.

_____ I will log out of and close the browser after each use of CDE data and reporting systems.

_____I will only access data in which I have received explicit written permissions from the data owner.

Handling Sensitive Data

_____ I will keep sensitive data on password-protected state-authorized computers.

_____ I will keep any printed files containing personally identifiable information in a locked location while unattended.

_____ I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.

_____ I will delete files containing sensitive data after working with them from my desktop, or move them to a secured CDE server.

Reporting & Data Sharing

_____ I will publish only aggregate data in groups no smaller than 16 children in public reports and only for valid state-level purposes including but not limited to: program evaluation, state/federal accountability, stakeholder requests for information, and public engagement presentations.

_____ I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

_____ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.

_____I will not transmit child/staff-level data externally unless explicitly authorized in writing by the data owner and Institutional Review Board representative when applicable (i.e. as part of a formal research study).

_____ I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or CDE's Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for CDE internal file transfer.

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the CDE Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

_____I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

Termination of Employment

_____I agree that upon the cessation of my employment from CDE, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of CDE without the prior written permission of the Chief Information Officer of CDE.

Print Name: _____ Signed: _____

Date: _____