

## Important Data Privacy Reminder

This document/file contains individual student education record data. You are receiving this information because you are a school official as defined by the [CSCU FERPA Notice and Directory Information Policy](#). As the recipient of this data, it is your responsibility to safeguard it and use it only for the purpose for which it was provided.

### Limited Use

In accordance with the [Family Educational Rights and Privacy Act \("FERPA"\)](#), student education records may only be shared without a student's consent under a few exceptions. One exception is that student education records may be shared with a school official for legitimate educational purposes. Generally, a school official has a legitimate educational purpose if the school official needs to review the student education record(s) in order to fulfill the school official's professional responsibilities. Putting this into practice means:

- Do not share this and other information from student education records with other school officials unless there is a clear legitimate educational purpose for doing so.
- Do not share this or other information from student education records outside of your institution without verifying that the recipient is authorized to receive it. In most cases, this would mean there is a written agreement governing data sharing or such transfer of student education records is authorized by applicable law.
- Immediately notify the CSCU Security Office at [Security@ct.edu](mailto:Security@ct.edu) if you know of or suspect a loss or misuse (by any means) of student education records, or you know of or suspect an inadvertent, unauthorized, and/or unlawful disclosure, processing, alteration, corruption, sale, rental, or destruction of student education records or other breach with respect to student education records.

### Safeguarding Education Record Data

To maintain confidentiality and minimize unauthorized access, you should use secure mechanisms to store and transmit individual level data – even to others within CSCU.

- Use a secure Microsoft TEAMS channel to transmit data.
- Apply password protection to data files and provide the password separately from the data.
- Encrypt email messages used to transmit student level data.
- Be careful with data files that contain pivot tables linked to individual level data.
- Keep data with [DCL3](#)\* information in the Protective Enclave.

### What are the consequences of violating FERPA?

- Suspension of employee or contractor access institution data
- Employee discipline, including possible dismissal or termination
- Possible federal and state enforcement agency investigations
- Loss of federal funding to the institution

In light of these consequences, access to student education records must be used responsibly. On-going training and communication are important.

If you have questions about what disclosure is permitted under FERPA, please contact CSCU Privacy Office at [CSCU-DataPrivacy@ct.edu](mailto:CSCU-DataPrivacy@ct.edu).

**Thank you for doing your part to safeguard student education records and protect student privacy.**

*\*DCL3 data are highly protected and include but are not limited to: SSN, bank account, credit/debit card, student financial aid data derived from the National Student Loan Data System (NSLDS), the Institutional Student Information Record (ISIR), or the Free Application for Federal Student Aid (FAFSA).*