	Student Data Access Policy	
	Responsible Administrative Unit: Registrar	**Policy Contact:** Registrar pmyskiw@mines.edu

1.0 BACKGROUND AND PURPOSE

Colorado School of Mines' (Mines) institutional data, including Student Data, must be managed and maintained consistent with state and federal law and relevant Mines policies, while ensuring that it is protected from unauthorized disclosure. The Policy defines the responsibilities of those employees who require access to Student Data in order to carry out their specifically assigned educational or administrative responsibilities.

Mines' handling of Student Data is in compliance with the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g, which generally prohibits the disclosure of education records other than public directory information, without the student's permission. FERPA does not require consent prior to disclosure to university employees in the process of carrying out their specifically assigned educational or administrative responsibilities, or to other school officials with legitimate educational interests. Please refer to the Mines FERPA policy here.

2.0 POLICY

Anyone using or processing Student Data must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data at all times, and is consistent with state and federal law, including FERPA. Student Data may be accessed, used and disclosed only in the performance of specifically assigned educational or administrative responsibilities, by school officials with legitimate educational interests, or in a manner otherwise consistent with Mines' FERPA Policy.

3.0 PROCEDURES

3.1 FERPA Training

All employees who require access to Student Data must complete the online FERPA training. Training must be refreshed every two years.

3.2 Agreement to Policies

Once the FERPA training is completed, data users must sign a FERPA agreement and acknowledge this Student Data Access Policy statement, and agree to comply with the following relevant Mines policies:
FERPA Policy
Administrative Data Policy
Data Classifications and Roles Definitions

3.3 Disclosure to Third Parties

Please remember that dissemination of general information to students must adhere to the Email Lists Policy. Even though access to email addresses maybe provided, only approved emails may be sent directly to students.

To ensure that Student Data is reported to outside agencies or any third party in compliance with FERPA and other applicable laws and policies:

- The Office of Institutional Research must be consulted for university-wide studies and use of any and all aggregate Student Data that is requested by all non-Mines entities. This includes data requested for third-party **surveys**, requests from outside **vendors**, **professional societies**, or **accrediting agencies**.
- The Office of the Registrar must be consulted for any data requested from third-parties that includes any detail about specific students at Mines (even directory information) such as media, marketers, non-profits, for profit businesses, sororities, fraternities, honor societies, parents, family members of students, and scholarship programs.
- Student Data needed for research and design of instructional programs by Mines faculty must be approved and supplied by the Assessment team in the Trefny Center.
- The Office of Legal Services must coordinate all responses to third-party requests for Student Data made through subpoenas or Colorado Open Records (CORA) requests.

3.4 Maintenance and storage of Student Data

- All Student Data taken from Banner/ODS via COGNOS and put into local spreadsheets, documents, or databases must be maintained on Mines campus computing networks made available to campus employees for work purposes that are protected by passwords and campus firewalls.
- Student Data may not be stored on local (C:) drives of work or personal laptops or desktop computers or unencrypted jump drives.
- In the event that a computer is stolen where private Student Data has been stored on a local (non-network) drive, the user is required to immediately contact either Campus Computing, Communications, and Information Technologies (CCIT) or the Registrar's Office in order to report the stolen data. The data in the stolen files will need to be identified and an assessment will be completed concerning official notification requirements for the purposes of FERPA or other necessary compliance with Federal or State laws.

4.0 Questions

Questions about this policy may be directed as follows:

Registrar's Office
Phone: 303-273-3200 or
E-mail: pmyskiw@mines.edu

Office of Legal Services
Phone: 303-273-3325

Office of Institutional Research
Phone: 303-273-3383
Email: tdouthit@mines.edu

Campus Computing, Communications, and Information Technologies (CCIT)
Phone: 303-273-3431

5.0 Compliance/Enforcement

Employees who violate this University policy may be subject to disciplinary action for misconduct and/or performance based on the administrative process appropriate to their employment.

6.0 Definitions

6.1 Student Data means education records of students as defined by FERPA, and includes those records that are (1) directly related to a student; and (2) maintained by Mines or a party acting for Mines. See [link to FERPA Policy].

7.0 HISTORY AND REVIEW CYCLE

The policy will be reviewed at least annually, or as needed by the Responsible Administrative Unit.
Last Issued: September 2019