The Mines’ Data Code of Conduct has been established as guiding principles for University employees who steward and/or handle Mines’ data.

A. **Data protection is the responsibility of the Mines’ community**

B. **The highest priority is to respect the person(s) behind the data**
   The person’s data belongs to the person. Employees responsible for the collection, maintenance, use, and dissemination of information about a person, are to comply with applicable laws and regulations.

C. **Attend to the downstream uses of data sets**
   Data should be used in ways consistent with the intentions and communications with the disclosing party. Consideration should be given to ensure downstream uses of data (including data provided to vendors and subcontractors) are appropriate and have been communicated with the disclosing party.

D. **Use data for the business purposes communicated to the person**
   The unsolicited use of data for purposes other than the purpose of origin is not allowed. Employees are not to seek out or use information relating to others for their own interest or advantage. The intentional violation of this rule may be cause for disciplinary action.

E. **Do not collect more data for the sake of collecting more data**
   Employees are not to require individuals to disclose information about themselves which is not necessary and relevant to the purposes of the University or to the particular function for which the employee is responsible.

F. **Disclose data as allowable**
   Employees are not to disclose information relating to individuals to unauthorized persons or entities. Even though some disclosures may be allowable, discretion should be used when disclosing data. The intentional disclosure of such information to such persons or agencies may be cause for disciplinary action.

G. **Assist with inquiries and requests timely**
   Employees are to make every reasonable effort to see that inquiries and requests by individuals for their personal records are responded to quickly, courteously, and without requiring the requester to repeat the inquiry to others unnecessarily. Employees are to assist individuals who seek information pertaining to themselves in making their inquiries sufficiently specific and descriptive so as to facilitate locating the records.

H. **Strive to match privacy and security safeguards with privacy and security expectations**
   Employees responsible for the maintenance of records are to take necessary precautions to assure that proper administrative, technical, and physical
Mines’ Data Code of Conduct

safeguards are established and followed in order to protect the confidentiality of records containing sensitive information.

I. **Employees should not keep information longer than necessary, as defined within University policy**

J. **Aspire to design practices that incorporate transparency, accountability, and auditability**
   Thinking ahead is key to success. Maximize transparency at the point of data collection can minimize more significant risks as the data travels through the process. As much as possible, the history of data sets should be auditable, including mechanisms for tracking the context of collection, methods of consent, the chain of responsibility, and assessments of quality and accuracy of the data.

K. **Data can be a tool of inclusion and exclusion**
   Not everyone is equally impacted by the processes of data collection, use, and disclosure. Mitigate any disparate impacts of personal data.

L. **Follow the law, but understand that the law is often a minimum bar**
   As technology changes rapidly, laws and regulations may fail to keep up at the same pace. Follow the law, and take it one step further to ensure the highest level of data ethics to comply with the spirit of the law as things change.

M. **Report any areas that may not comply with Mines’ policies and procedures**
   In the event of data protection incidents, the incident mitigation must be initiated immediately. The Privacy Compliance Director or the Chief Information Security Officer will investigate and notify data subjects and regulators, as required.