Purpose

This document is an extension of the Colby College Information Systems and Data Security policy, which includes several references to the term 'sensitive information.' For the purposes of information and data security, 'sensitive information' is broadly defined as:

Any information for which loss, alteration, misuse or disclosure could adversely affect the interests of the College or its administration, faculty, staff, students, applicants or relations therein. By default, this includes any such information held by the College whether or not such information is subject to legal protections or restrictions.

Specific examples of sensitive data are:

- Social Security numbers (SSNs)
- Credit card or other financial account numbers
- Drivers license numbers
- Personally identifiable information pertaining to individuals (students, applicants, parental/familial relatives, alumni, donors, current and retired faculty and staff)
- Academic data such as grades and enrollment data (as specified under FERPA)
- Medical and health data
- Proprietary and/or copyrighted data, such as research data and publications
- Confidential legal or financial data

Under the Information Systems and Data Security policy, it is the responsibility of each individual with access to sensitive data to safeguard these resources by adhering to all established laws and policies as well as any relevant ITS data security procedures with regard to safe handling, access control and electronic (network) transmission.

Under the Colby College Code of Ethics for Information Technology, all personal data is treated as private and confidential. This includes all sensitive data but may also include personal communication or electronic files and/or records. ITS staff, system administrators and handlers of sensitive information are expected to treat all electronic files and network communication (including email and general Internet use) as private and confidential.