DATA STEWARDSHIP
PRIVACY AND SENSITIVITY OF DATA MAINTAINED BY THE COLLEGE

GUIDELINES

Data maintained by Pomona College are subject to various laws and regulations that protect the privacy of information that includes personal identifiers – data elements or reports that include information connected to individuals (students, faculty, staff, alumni, donors, etc.) whose identity can be revealed or discerned from college sources. The laws include, but are not limited to:

FERPA (Family Educational Rights and Privacy Act)
HIPAA (Health Insurance Portability and Accountability Act)
GLBA (Gramm Leach Bliley Act)

Certain types of summary data (i.e., not involving identification of any individuals) are maintained by the college, and similar data are received by the college from data-sharing consortia such as COFHE. Some of these data are considered “confidential” or “proprietary” for reasons of institutional policy or inter-institutional agreement, and must also be protected from unauthorized release or distribution. Such data are the subject of separate guidelines and are not addressed in this document, the focus of which is PII (Personally Identifiable Information).

PII is defined by the National Institute of Standards and Technology as:

"...any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

In the context of Pomona College, this definition includes data that may be prioritized according to their level of “Sensitivity”. The designations of data sensitivity listed below are relevant for data stored and maintained by college employees in electronic or paper form, and also for data stored on “cloud” and similar hosted information services. It is essential that all college employees who have access to such data follow college guidelines about security procedures, including locking storage areas, encrypting data that are transmitted or carried on mobile devices, monitoring access privileges to online data resources, and enforcing security-related contractual arrangements with outside vendors.

HIGHEST SENSITIVITY DATA / RESTRICTED

- Social Security Number or Driver’s License Number
- Contact information (except as permitted by FERPA or by the individual)
- Birthdate, previous names, identity of parents or other relatives, or other information that might be traced to a specific individual
- Credit card, debit card, bank account number, and data such as “mother’s maiden name” commonly used for verification of identification
- Health or health insurance information (except as permitted by FERPA for emergency purposes)
- Student academic record, as defined by FERPA
- Employee salary, performance review, or disciplinary records
- Donor/Gift records

Data in these categories must be afforded the highest level of protection against release to any unauthorized individual or entity. This protection must include:

- Procedures to secure all files and reports maintained in hard copy form
- Practices that protect against inadvertent exposure of data at workstations
- Implementation of “best practice” procedures for permissions and access privileges to electronic data sources maintained by the college
- Procedures to assure that transmission of such data across data networks (including email, backup storage, etc.) are encrypted
- Policies requiring anyone carrying such data on mobile devices to implement password-controlled security protections on these devices
- Agreements with “cloud” or other “third-party” vendors or contractors that ensure the highest level of security protection for any highly sensitive data transmitted to their systems, clarity about "ownership" of such data, guarantees of "disposal" of such data upon termination of any contract, and appropriate levels of indemnification of the College for any unauthorized release of such data from systems not controlled by Pomona College

**MEDIUM SENSITIVITY DATA / CONFIDENTIAL**

- Information designated by FERPA as “directory information” or for which the individual has implicitly or explicitly authorized release to others (e.g., alumni providing email contact information for an online directory)
- All other FERPA-protected information not include in the HIGHEST SENSITIVITY category
- Verification of an individual’s employment at Pomona College
- Other “personal” but not highly sensitive data

Release of data in these categories will not expose the College to liability and will not violate any laws, but may violate reasonable expectations and understandings that individuals have in their relationship with the College. Decisions about such releases are made thoughtfully and intentionally by responsible individuals in the functional areas that have primary oversight of the data. Agreements with “cloud” or other “third-party” vendors or contractors must ensure that the data are never released to or accessed by others without the consent of the College.

**LOW SENSITIVITY DATA / UNRESTRICTED**

Data that are very unlikely to be identifiable or that are broadly available from public sources are considered LOW SENSITIVITY and do not require special protections, but might still be subject to College policies that discourage or prohibit the College from functioning as a source of such data. Examples might be contact information for individuals associated with the College where that contact information is also available from other public sources, and information about affiliations and/or activities of individuals, such as club memberships, activities, leadership positions, etc.