Data Management Policy

Overview

The Office of Institutional Effectiveness (OIE) is committed to data stewardship. Data stewardship refers to the responsible oversight and management of data that are stored, collected, and analyzed by OIE. Data stewardship ensures that the integrity and quality of institutional data are maintained, and also protects the confidentiality and rights of research participants, students, faculty, and staff. Institutional data are university assets; thus, it is vital that data are guarded against unauthorized alteration or inappropriate usage in accordance with university policies, and federal and state laws. This is accomplished through appropriate usage of data, as stated in this policy.

The following areas are discussed in this policy:

- Data classification
- Data permissions/requests
- OIE analysis and reporting

This policy establishes standards for assuring data integrity, while also ensuring that OIE effectively serves the needs the of Pepperdine community. OIE believes data should be safeguarded to maintain confidentiality and privacy; however, such safeguards are weighed and balanced with the needs of the University to conduct its business and effectively serve its students, faculty, and staff.

Data Classification

Pepperdine University is the owner of all OIE-related data. University data are classified into three categories: restricted, confidential, and public. The table below summarizes these categories.

Data category	OIE Usage	Institutional risk level	Description	Examples
Restricted	Rare	High	Data contain highly sensitive information and personal identifiers. Unauthorized access to these data could seriously impact Pepperdine, OIE, and/or the persons with whom data are associated.	▪ Social security numbers ▪ Credit card numbers ▪ Protected health information (HIPPA-covered records)
Confidential	Often	Medium	Data contain sensitive information and/or personal identifiers.	▪ Grades ▪ FERPA-covered records ▪ Human resource data ▪ Research data ▪ Campus ID number ▪ Survey data
Public	Often	None	All publically available data.	▪ Enrollment data ▪ FERPA directory information ▪ IPEDS survey data ▪ Common Data Set

OIE primarily handles confidential data. In the rare instances in which OIE handles restricted data, the Director of Institutional Research and/or Associate Provost oversees and manages this process in order to protect confidentiality.

For more information, view Pepperdine University's Information Classification and Protection Policy, Family Educational Rights and Privacy Act (FERPA), and the Health Care Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and Security Rule.

Data Permissions/Requests

All external requests for data (i.e., outside of OIE, but still within the Pepperdine community) are submitted through an OIE Data Request Form, in which individuals/departments requesting data are asked to provide information on their data-related needs, purposes for the request, and agreement with OIE's data waiver. Any data reports provided by OIE must be used for Pepperdine University needs and purposes. Personal use of OIE data and/or reports are prohibited.

The following three statements summarize data request- and report-related items that are prohibited by OIE:

1. OIE *does not* provide any raw data files in order to protect individuals' confidentiality and privacy.
2. OIE *does not* provide contact information of Pepperdine students, faculty, or staff for mass emails, listservs, or other solicitation-related requests in order to abide by FERPA guidelines. All such requests will be referred out to the Registrar or Human Resources.
3. OIE *does not* disaggregate confidential data with limited counts/cases, specifically for any demographic sub-population with fewer than 20 cases, and programs/majors/divisions with fewer than 10 cases.

Individuals/departments requesting data are expected to take measures to safeguard data. This includes:

- Securely storing data on University encrypted drives or computers.
  - Password protect data files.
  - Store data on University computers or servers.
  - Do not share any data through unsecure email.
  - Do not share data results with the press (radio, television, print, or electronic media) without appropriate University authorization.
- Safely disposing data.
  - Destroy OIE data files and/or reports within one-year of receipt, unless needed for longitudinal purposes. Destroy files in a manner that prevents re-creation.

All data requests will be handled on a case-by-case basis. OIE staff will work to meet the needs of those requesting data, while ensuring data stewardship and privacy.

OIE Analysis and Reporting

Data analyses are conducted by OIE's institutional research (IR) staff. IR staff are required to complete human subjects certification, and must have an educational background, experience, and/or degree in higher education or social science.

OIE analyses and reports are predominantly sourced from the following:

- *Student and HR census*—Census data are based on a snapshot of enrollment at fifth week for the student census (fall and spring terms), and faculty/staff employment as of November 1st for the HR census. Data are generally provided as exports, visualizations, reports, and infographics.
- *Survey data*—Data are based on student, alumni, and faculty surveys. OIE generally administers nine surveys each year to different sub-populations (see OIE's survey schedule)

Most OIE reporting is based on census data, due to the federal reporting requirements by the National Center for Education Statistics (NCES) Integrated Post-Secondary Education Data System (IPEDS). *IPEDS reporting is mandatory for all institutions that receive federal funding.* Requests that are not based on the above data sources will be referred to other campus departments.

All OIE-related data are stored on encrypted desktop computers that are only accessible to OIE staff.

****

OIE reserves the right to make adjustments to this policy in order to safeguard and protect participant confidentiality, and to ensure data integrity.