OIE Office of Institutional Effectiveness
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 all 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
- Access
- Permissions/Requests for Data
- OIE Analysis and Reporting
- OIE Data Storage

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

Data Classification
OIE data are classified into three categories: restricted, confidential, and public. The table below summarizes these categories.

Data category	Institutional risk level	Description	Examples
Restricted	High	Data that contain highly sensitive information and personal identifiers. Unauthorized access to this type of data could seriously impact Pepperdine University, OIE, and/or the persons with whom data are associated.	• Social security numbers • Credit card numbers • Protected health information (HIPPA-covered records)
Confidential	Medium	Data that contain sensitive information and/or personal identifiers.	• Grades • FERPA-covered records • Human resource data • Research data • Campus ID number • Survey data
Public	None	All publically available data.	• Census data • FERPA directory information

OIE primarily handles confidential data. In the rare instances in which OIE handles restricted data, the Director of Institutional Research 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.

Access

Pepperdine University is the data owner. Data are provided only to members of Pepperdine University, which include Pepperdine staff, faculty, students, administration, and departments.

Permissions/Requests for Data

All external (i.e., outside of OIE, but still within Pepperdine) requests for data are submitted through a data request form, as OIE tracks all requests for data. Individuals/departments requesting data are asked to provide the following:

- Contact information: name, title, department or office, phone
- Type of request: direct institutional research data (e.g., student grades, retention, graduation rates), indirect institutional research data (e.g., national survey data, data collected by OIE), or research request
- Specific need: variables desired, analyses desired (if applicable), time range, and other pertinent information
- Purpose/usage of data
- Agreement to abide by OIE's data management policy, particularly with securing and disposing data
- OIE staff person whom request should be directed (if applicable)

Data provided by OIE must be used for Pepperdine University needs and purposes. Personal use of OIE data are prohibited. *OIE does not provide any raw data files in order to protect individuals' confidentiality and privacy*.

Individuals/departments requesting data are expected to take measures to safeguard data and will be required to sign a Data Request Agreement. This includes:

- Securely storing data on University encrypted drives or computers.
    - Password protect data files and properly backing them up.
    - Do not store data on computers or servers outside of the University unless permission to do so has been granted by OIE and/or Pepperdine's IRB.
    - Take extra precautions when storing highly sensitive or restricted data, and do not store these types of data on computers or servers outside of Pepperdine University.
    - Sensitive and restricted data should not be redistributed
    - 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.
    - Data files shared outside of OIE should be destroyed within one-year of receipt. Data should be destroyed in a manner that prevents re-creation. If data needs extend beyond one-year, OIE should be notified in writing.
    - Shred any printouts of sensitive data.

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

OIE Analysis & Reporting

Analyses conducted by OIE staff are done in SPSS, Stata, and Excel. There are two main data reports provided by OIE; reports based on census/student success data, and reports based on educational survey data.

Census and student success data—These data are provided by OIE's Director of Institutional Research. Data are primarily reported as frequencies, measures of central tendency (e.g., means, medians), and percentages. In most cases, data are reported in aggregate form. Disaggregated data are provided at the discretion of the Director of Institutional Research in order to ensure data integrity.

Educational survey data—These data are provided by OIE's Associate Director of Institutional Research, and are also primarily in aggregate form. When data are disaggregated, reports/analytics are not provided for any disaggregated group of 10 or fewer cases; however, in some instances demographic data (e.g., ethnicity, gender) are not provided for cases with fewer than 20. Missing data are not included in these analyses.

OIE Data Storage

OIE stores data 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.