Reporting Standards & Practices

Reporting standards and practices in the University of Maine System (UMS) are decentralized, meaning that each campus is responsible for their own institutional research and reporting needs. The System Office coordinates media and legislative requests requiring data from the seven UMS institutions. Reporting at each UMS institution covers an extensive array of categories, such as admissions, student records, financial aid, curriculum assessment, enrollment management, human resources, finance, facilities, and alumni relations. Consistent reporting requires following agreed upon data definitions. Organizations like the National Center for Education Statistics have a set of definitions as part of the Integrated Post-Secondary Education Data System (IPEDS). The Common Education Data Standards (CEDS) project allows colleges and universities to develop shared standards and definitions among a key set of data elements. In addition, effective practices for data reporting may be provided by professional associations, such as the Association for Institutional Research (also see NEAIR for the New England region), Association of American Universities Data Exchange, Higher Education Data Sharing Consortium, Consortium on Financing Higher Education, and the College and University Professional Association for Human Resources. Institutional researchers must follow the appropriate governmental regulations and institutional policies for handling data.

Contents

- Data Definitions
- Data Security and Sensitivity
- Government Regulations
- UMS Policies and Procedures

Data Definitions

Definitions for terms provide important context for understanding information and specific guidance on how each data element should be used. They give details about the structure of data elements and details about the format of data. Examples of how data definitions are useful for include units of measurement, time-frames, and names for categories. The most commonly used data definitions for institutional research and reporting are related to student enrollment, records, and admissions. (for more, see Data Definitions)

Data Security and Sensitivity

Users given access to the data must adhere to the following principles:

1. Users must understand the meaning, purpose, and interpretation of the underlying data.
2. Users must ensure the accurate and responsible presentation of information derived from the data.
4. Unauthorized or inappropriate destruction, modification, or disclosure of information by a user may result in denial of access or may be cause for disciplinary action.

In all cases, information access and disclosure should only occur as part of the required exercise of one’s duties as University employees. In addition, as described in the Family Educational Rights and Privacy Act section, any information from a student’s Education Record cannot be released except in certain specified situations. In some cases it is permissible to disclose Directory Information if there is a legitimate educational interest and the disclosure is necessary to fulfill one’s job responsibilities. Directory Information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to:

1. Student’s name
2. Address (excluding email address)
3. Telephone number
4. Date and place of birth
5. Honors and awards received
6. Dates of attendance
7. Electronic mail address
8. Photograph
9. Major field of study
10. Grade level
11. Enrollment status (e.g., undergraduate or graduate; full-time or part-time)
12. Participation in officially recognized activities and sports
13. Weight and height of members of athletic teams
14. Degrees
15. The most recent educational agency or institution attended.
The following information should generally be considered sensitive in nature and should only be disclosed when there is a legitimate educational interest and the disclosure is necessary to fulfill one’s job responsibilities.

1. Social Security Number
2. Combination of Name and Employee ID
3. Gender
4. Ethnicity
5. Marital status
6. Religious preference
7. Veteran status
8. Disability information
9. Class schedule
10. Academic history/grades
11. Medical records including immunizations
12. Employer information
13. All Bursar information
14. All Financial aid information except some scholarship information
15. Employee benefit information
16. Tax Information
17. Visa status
18. User names and passwords

Government Regulations

Laws pertaining to the use of data vary from state to state. The Federal laws most institutional researchers and data users will need to know pertain to a few major laws.

- Federal Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Genetic Information Nondiscrimination Act (GINA)
- Fair and Accurate Credit Transactions Act (FACTA)

FERPA is the law most related to the use of student data, placing restrictions on what may or may not be reported publicly. HIPAA is a law restricting the use of most data pertaining to medical and health related information. GINA regulates how genetic information may be used. FACTA protects certain credit related and financial data.

UMS Policies and Procedures

The policy regarding the appropriate use of data for information security purposes is covered under Administrative Practice Letter (APL) VI-C - Information Security. In addition to UMS policies and procedures, all state and federal laws must be followed when using UMS data.