

Data Governance

Institutional Policies & Procedures

Institutional Research, Analysis, & Planning

March 2017

Data Governance: Institutional Policies and Procedures

An online version can be found at www.bates.edu/research/data-governance-at-bates-college/

Produced by:

Institutional Research, Analysis & Planning

2 Lane Hall
2 Andrews Road
Lewiston, Maine 04240

207-786-8211

Contents

- Basic Data Sharing Principles 1
- Policies and Procedures 2
 - Data Access 2
- Classification of College Data 3
 - Classification of Data 3
 - Classification Levels 3
- Roles Required to Govern Data 4
- Data Administrator Contact List 5

Basic Data Sharing Principles

The purpose data governance is to establish guidelines that ensure that institutional data is both secure and available to those who should have access to it. As Bates continues to grow in its commitment to a culture of data-informed decision-making, it is our hope that the policies and procedures delineated below serve as a useful resource to data stewards, users, and seekers alike.

College records exist for the purposes of the business of the college. Requests for data outside of that use are subject to the following considerations:

- Data sensitivity
- Compelling policy interest
- Reputational risk
- Confidentiality
- Anonymity to the extent possible
- IRB Approval

Policies and Procedures

Critical to the ongoing work of the college, responsible stewardship of Bates college data is required in order to ensure those with official educational or administrative responsibilities are able to access and rely on the accuracy and integrity of the data. Data stewards are expected to comply with the following data policies and manage data within their care in a manner that is consistent with legal, ethical, and practical considerations.

Data Access

Data access will be granted to those with legitimate educational interest to the data upon approval of the appropriate Data Steward and may require approval of a Data Trustee. This may only comprise individuals who are employees or volunteers of the institution needing the data to perform assigned duties.

Improper release, maintenance or disposal of college data may be damaging to the college community and exposes Bates to significant risk and possible legal action. Those granted access to college data must agree to the following guidelines.

- Maintenance of data must strictly adhere to the policies and procedures of Bates College. Data may not be altered or changed except in the usual course of business.
- Data may not be released to third parties or others at the college who do not have access to the data without the consent of the appropriate Data Steward/Administrator and must always be done in compliance with FERPA.
- Access to and use of data is restricted to the scope of an individual's work. Data should not be viewed or analyzed for purposes outside of official business.
- Data Users, as defined in the roles policy, may not grant access to data. If data needs to be shared with others, the appropriate data steward needs to authorize access to those data.

All security and computer use policies must be adhered to: see the [Bates website](#). Do not compromise Bates security by sharing passwords or other sensitive information.

Classification of College Data

Classification of Data

Accurate classification provides the basis to apply an appropriate level of security to college data. All College data are classified into levels of sensitivity to provide a basis for understanding and managing college data. These classifications take into account the legal protections (by statute, regulation, or by the data subject's choice), contractual agreements, ethical considerations, or strategic or proprietary worth. They also consider the application of "prudent stewardship," where there is no reason to protect the data other than to reduce the possibility of harm or embarrassment to individuals or to the institution.

The classification level assigned to data will guide Data Trustees, Data Stewards, Data Administrators, and Data Users in the security protections and access authorization mechanisms appropriate for those data. Such categorization encourages the discussion and subsequent full understanding of the nature of the data being displayed or manipulated.

By default, all institutional data will be designated as "Internal." College employees will have access to the data for use in the conduct of college business.

Classification Levels

Public Data (low level of sensitivity)

Access to "Public" institutional data may be granted to any requester. Public data are not considered confidential. The integrity of Public data must be protected, and the appropriate owner must authorize replication of the data. Examples include: institutional statistics that appear in publications, academic course descriptions, Common Data Set, and Bates Facts.

* Information contained in the Bates Online Directory is technically "Directory Information" under FERPA (can be released without consent) but some information is password protected and should not be considered "Public."

Internal Data (moderate level of sensitivity)

This classification applies to information protected due to proprietary, ethical, or privacy considerations, even though there may not be a direct statutory, regulatory, or common-law basis for requiring this protection. Internal data is restricted to personnel designated by the College who have a legitimate business purpose for accessing such data. Examples include: institutional survey data, and enrollment projection data.

Restricted Data (highest level of sensitivity)

This classification applies to information protected by statutes, policies, or regulations. This level also represents information that isn't by default protected by legal statute, but for which the Data Administrator has exercised his or her right to restrict access. Examples include: PII - Personally identifiable information (SSN, driver's license, bank account numbers), salary data, academic record data (unit level) and financial aid data.

Roles Required to Govern Data

Several roles and responsibilities govern the management of, access to and accountability for institutional data.

Data Governance Committee

This committee is comprised of functional data stewards from across all functions and departments of the College.

Data Trustees

Data Trustees are senior college officials (e.g., vice presidents) or their designees who have planning, policy-level and management responsibility for data within their functional areas.

Data Stewards

Data Stewards are college officials who have direct operational-level responsibility for the management of one or more types of institutional data. Data Stewards are assigned by the Data Trustee and are generally associate vice presidents, directors or managers.

Data Administrators

Data Administrators are individuals (outside of ILS) who are responsible for data collection and management and who have been granted authority to grant internal access to data from their functional area by the Data Steward and/or Data Trustees.

Data Users

Data Users are college units or individual college community members who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the college; this access is granted solely for the conduct of college business.

Below is the organizational scheme for trustees and stewards by administrative data area. See contact list below for designated data administrators.

Administrative Data Area	Data Trustee	Data Steward
Admission	Dean of Admission & Financial Aid	Admission Research Analyst & Information Systems Manager
Advancement & Alumni	VP for College Advancement	Senior Director of Advancement Services
Finance	VP for Finance & Administration / Treasurer	Controller
Financial Aid	Dean of Admission & Financial Aid	Director of Student Financial Services
Human Resources (Faculty/Staff)	VP for Finance & Administration / Treasurer	Assistant VP of Human Resources
Information & Library Services	VP for Information & Library Services and Librarian	Director of Systems Development & Integration (IS) Assoc. College Librarian for Systems & Bibliographic Services
Institutional Statistics & Analytical	President	Director of Institutional Research, Analysis, & Planning
Student Affairs	VP for Student Affairs & Dean of Students	VP for Student Affairs & Dean of Students
Student Enrollment & Academic Affairs	VP for Academic Affairs & Dean of the Faculty	Registrar

Data Administrator Contact List

Admission Data

Contact Deborah Obptande: dobptand@bates.edu

Advancement & Alumni Data

Contact Patricia Ayers-Miller: payersmi@bates.edu
Jeremy Braz: jbraz@bates.edu

Finance Data

Contact Natalie Williamson: nwilliam@bates.edu

Financial Aid Data

Contact Wendy Glass: wglass@bates.edu

Human Resources (Faculty/Staff) Data

Contact Sarah Bernard: sbernard@bates.edu

Information & Library Services Data

Contact Eileen Zimmerman: ezimmerm@bates.edu (Systems Development and Integration)
Sharon Saunders: ssaunder@bates.edu (Systems and Bibliographic Services)

Institutional Statistics & Analytical Data

Contact Ann Marie Russell: arussell@bates.edu

Student Affairs Data

Contact Mary Meserve: mmeserve@bates.edu
Vincent Bellina: vbellina@bates.edu

Student Enrollment & Academic Affairs Data

Contact Mary Meserve: mmeserve@bates.edu
Robert Leighton: rleighton@bates.edu
Megan McHenry: mmchenry@bates.edu
Matt Duvall: mduvall@bates.edu

Institutional Research, Analysis, & Planning

March 2017