Applies to: *Faculty (including part-time and visiting faculty), staff and students (including graduate/undergraduate student workers and graduate assistants) employed by the University This policy continues to apply to individuals on sabbatical, other leaves or while visiting other institutions*

1. Policy

Issued: August 2023
Last Revised: August 2023
Last Reviewed: January 2026

2. Policy Purpose

The policy fits into the University IT governance framework. The Data Governance Advisory committee maintains this policy to insure the integrity, privacy and security of the University Data. The Process Team Leads serve as the governing body to oversee this policy per the IT Governance Policy.

3. Scope and Application

This policy covers all University data. It supersedes any other data policy. This policy replaced the Data Classification Policy.

4. Definitions

Data Governance is a cooperative effort which depends on the collaboration between key University stakeholders, who provide critical expertise and perspectives related to specific aspects of data management.

Term	Definition
Executive Council	The president's cabinet serves as the executive council and sponsors the Data Governance Program and its role in managing, protecting, and ensuring the integrity of University Data. They resolve conflicts escalated by the Data Governance Advisory committee.
Data Trustees	Data trustees assigned by the President's cabinet provide a strategic perspective on data governance. They have decision-making authority regarding the data associated with particular business Domains. They have the primary responsibility to ensure that the University is following its Data Governance Policy and is in compliance with federal and state laws and regulations. They identify the data classification (sensitivity) of data. Data Trustees are responsible for engaging affected offices and

	the user community before formulating changes or additions to this Data Governance Policy.
Data Governance Committee	Data Governance Advisory Committee is the collection of Data Trustees. It collectively advises the Executive Council. It defines, maintains, and publishes component policies, procedures, and processes to address data access and use, data definitions, data privacy, and data security. The Council works through consensus to resolve conflicts regarding access and data-quality controls where data overlap between multiple functional units. A member of ITS serves on the Council of Data Trustee ex-officio.
Data Ownership	Rivier University is the institutional data owner. **Vice Presidents, as divisional leaders, hold primary responsibility for the data associated with their functional areas and therefore serve as Data Owners.** They may delegate day-to-day data stewardship responsibilities to units, departments, or designated Data Stewards.
Data Administration	Responsibility for the activities of data administration is shared among the Data Managers, Data Custodians, Chief Information Officer and designee.
Data Stewards/ Managers	University officials who have planning and policy-level responsibilities for data in their functional areas are considered Data Managers. The Data Managers, as a group, are responsible for recommending policies, establishing procedures and guidelines for University--wide data administration activities, and training of Data Users on the proper handling of data. Data Managers, as individuals, have operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data. Data managers are responsible for developing and applying standards for the management of institutional data, and for ensuring that Data Users are appropriately informed of security obligations associated with their data access. For historical reasons – because data and the responsibility for data have traditionally been organized along functional or subject-area boundaries – the Data Managers are established according to this same subject-area organizing principle. The Data Group – Data Governance Committee (a group of data managers) meets on a regular basis.
Data Custodian	Data Custodians are responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by Data Managers or their designees (usually the data managers), and implementing and administering controls over the information. In many cases at Rivier University the role of Data Custodian is a shared responsibility with the IT Department being responsible for physical security support (secure facility, backup and recovery) and the applicable Data Manager having responsibility for access and control over the information.
Data Users	Data Users can view, copy or download institutional data as part of their assigned duties or in fulfillment of their role within the Rivier

	community. All Data Users have an obligation to understand the security responsibilities associated with their level of data access.
Information Security Officer	University official who has oversight responsibility for the University's data security program as well as compliance with relevant regulations, security policies, standards and guidelines. At Rivier University this is part of the role of the Chief Information Officer.
Personal Identifiable Information (PII)	II is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., ..
Protected Health Information	"Protected Health Information" or PHI is all individually identifiable information that relates to the health or health care of an individual and is protected under federal or state law.
Privacy Officer	University official who has oversight responsibility for the University's privacy program as well as compliance with relevant regulations, privacy policies, standards and guidelines. At Rivier University this is part of the role of the Chief Information Officer.
Regulation Monitors	University officials who have oversight responsibility for one or more regulations. Regulation monitors stay abreast of updates to their respective regulations, ensure policies are up to date and notify the Information Security Officer and Data Managers about changes. The Policy group meets on a regular basis.
Student Records	"Student Records" are those that are required to be maintained as non-public by the Family Educational Rights and Privacy Act (FERPA). Student Records include Rivier-held student transcripts (official and unofficial), and Rivier-held records related to (i) academic advising, (ii) health/disability, (iii) academic probation and/or suspension, (iv) conduct (including disciplinary actions), and (v) directory information maintained by the Registrar's Office and requested to be kept confidential by the student. Applications for student admission are not considered to be Student Records unless and until the student attends Rivier University.
Qualified Machine	A "Qualified Machine" is a computing device located in a secure facility or remote that is managed by IT or has access control protections that meet Rivier's IT standards.
Computing Equipment	"Computing Equipment" is any Rivier or non-Rivier desktop, laptop, or portable device or system.

5. Policy Details

Rivier University takes seriously its commitment to respect and protect the privacy of its students, alumni, faculty, staff, parents and friends, as well as to protect the confidentiality of information important to the University's academic and research mission. The University recognizes that the value of its data resources lies in their appropriate and widespread use. It is not the purpose of this policy to create unnecessary restrictions to data access or use for those individuals who use the data in support of university business or academic pursuits.

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with data value, sensitivity, and risk. To implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data, data should be classified into one of the following categories:

- **Confidential** - Data which is legally regulated and data that would provide access to confidential or restricted data.
- **Restricted** - Data which the Data Managers have decided NOT to publish or make public and data protected by contractual obligations.
- **Public** - Data which there is no expectation for privacy or confidentiality.

Confidential data and restricted data will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business or research functions of the University, result in financial loss, or violate law, policy or University contracts. Security measures for data are set by the Data Custodian, working in cooperation with the Information Security Officer, Information Technology Services and the respective Data Managers. The table below outlines the criteria used to determine which data classification is appropriate for a piece of data or information system.

	Confidential (highest, most sensitive)	**Restricted (moderate level of sensitivity)**	**Public (low level of sensitivity)**
Description	Data which is legally regulated; and data that would provide access to confidential or restricted data.	Data which the data managers have not decided to publish or make public; and data protected by contractual obligations.	Data for which there is no expectation for privacy or confidentiality.
Legal requirements	Protection of data is required by law.	Protection of data is at the discretion of the owner or custodian.	Protection of data is at the discretion of the owner or custodian
Reputation risk	High	Medium	Low
Data Access and Control	Legal, ethical, or other constraints prevent access without specific authorization. Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements.	May be accessed by Rivier University employees and non-employees who have a business "need to know."	No access restrictions. Data is available for public access.
Transmission	Transmission of Confidential data through any non-Rivier network or Rivier guest network is prohibited (e.g.	Transmission of Restricted data through any non-Rivier network or Rivier guest network is	No encryption or other protection is required for public data; however, care should

	Internet). Transmission through any non-encrypted electronic messaging system (i.e. instant messaging, text messaging) is also prohibited.	strongly discouraged. Third party email services are not appropriate for transmitting Restricted data.	always be taken to use all University information appropriately.
Storage	Storage of Confidential data is prohibited on Non-qualified Machines and Computing Equipment unless approved by the Information Security Officer or designee. If approved, IT approved encryption may be required.	Level of required protection of Restricted data is either pursuant to Rivier policy or at the discretion of the owner or custodian of the information. If appropriate level of protection is not known, check with Information Security Officer or designee before storing Restricted information unencrypted.	No encryption or other protection is required for public data; however, care should always be taken to use all University information appropriately.
Documented Backup and Recovery Procedures	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are not necessary, but strongly encouraged.	Documented Backup and Recovery Procedures are not necessary, but strongly encouraged.
Documented Data Retention Policy	Documented data retention policy is required.	Documented data retention policy is required.	Documented data retention policy is not required, but strongly encouraged.
Audit Controls	Data Managers and Data Custodians with responsibility for Confidential data must actively monitor and review their systems and procedures for potential misuse and/or unauthorized access. They are also required to submit an update on at least an annual basis to the Information Security Officer or designee outlining departmental security practices and training participation.	Data Managers and Data Custodians with responsibility for Restricted data must periodically monitor and review their systems and procedures for potential misuse and/or unauthorized access.	No audit controls are required.

Examples	**Information resources with access to Confidential data (username and password).** **Student Data not included in directory information. This includes:** - Loan or scholarship information - Payment history - Student tuition bills - Student financial services information - Financial Aid awards - Class Lists or enrollment information - Transcripts; grade reports - Notes on class work including BLC and tutoring notes - Disciplinary action * - Housing information - Athletics or department recruiting information **Personal Identifiable Information (PII):** - Social Security Number - Driver's license - State ID card - Passport number Last name, and first name or initial, with any one of following: - Financial account (checking, savings, brokerage, CD. . .), credit card, or debit card numbers - Date of birth **Protected Health Information (PHI) *** - Health Status	**Personal/Employee Data** - Rivier ID number - Income information * - Payroll information * - Personnel records, performance Reviews, benefit information - Race, ethnicity, and/or nationality - Gender **Business/Financial Data** - Financial transactions which do not include regulated/confidential data - Information covered by non-disclosure agreements - Contracts – that don't contain PII - Credit reports - Assets/Net Worth - Records on spending and borrowing **Academic / Research Information** - Library transactions (e.g., catalog, circulation, acquisitions) - Unpublished research or research detail / results that are not regulated/confidential data - Non-anonymous faculty course evaluations - Private funding information - Human subject information **Anonymous Donor Information**	**Certain directory/contact information not designated by the owner as private.** - Name - Addresses (campus and home) - Email address - Listed telephone number(s) - Degrees, honors and awards - Most recent previous educational institution attended - Major field of study - Dates of current employment, position(s) - ID card photographs for institutional use Specific for students: - Class year - Participation in campus activities and sports - Weight and height (athletics) - Dates of attendance - Status **Business Data** - Campus maps - Job postings - List of publications (published research)

	- Healthcare treatment - Healthcare payment **Personal/Employee Data** - Worker's compensation or disability claims **Business/Financial Data** - Credit card numbers with/without expiration dates - Bank or brokerage account numbers - Purchasing card (P-card) numbers - Social Security or other Taxpayer ID numbers - Loan information - Wire Transfer Information	Last name, first name or initial (and/or name of organization if applicable) with any of the following: - Gift information, including amount and purpose of commitment **Other Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any of the following: - Telephone/fax numbers - E-Mail, URLs - Employment information - Family information (spouse(s)/partner/ guardian/children/ grandchildren, etc.) - Medical information **Management Data** - Detailed annual budget information - Conflict of Interest Disclosures - University's investment information **Systems/Log Data** - Server Event Logs * Exceptions apply	

6. Procedures

Each Data Steward is responsible for managing the procedures to maintain the system. When making changes to a process, the Data Stewart is responsible for sharing changes with the group to manage the impact the change may have on another department.

Procedures
Onboarding Procedure

User Access Rights Review

7. Forms

See department procedures.

8. Responsibilities

Division/ Department/ Domain	Position or Office	Responsibilities	Colleague Module
Academic Affairs	Registrar	Data Steward/ Manager	Student, Core, Curriculum, Faculty, Registrar
	Director of Institutional Research	Data Steward/ Manager	
	Global Engagement	Data Steward/ Manager	
	Director of Academic Advising	Data Steward/ Manager	
Enrollment	Admissions – Asst. VP for Enrollment Operations and Reporting	Data Steward/ Manager	Student, Core, Admissions
Finance	Vice President	Data Steward/ Manager	
	Controller	Data Steward/ Manager	Chart of Accounts, General Ledger, Accounts Payable
	Director of Human Resources	Data Steward/ Manager	Student, Core, Human Resources, Payroll
	Director of Student Accounts	Data Steward/ Manager	Student, Core, Student Accounts Receivable
	Director of Financial Aid	Data Steward/ Manager	Student, Core, Financial Aid
Advancement	Vice President	Data Steward/ Manager	Student, Core, CRMAdvance
	Director of Advancement Services	Data Steward/ Manager	
Student Experience	Assistant Vice President for Student Affairs	Data Steward/ Manager	
Information Technology	CIO	Data Steward/ Manager	

	Director of Enterprise Applications	Data Steward/ Manager	
	Business Reporting Analysts	Data Steward/ Manager	

9. Related Information

Related Policy
IT Governance Structure
Privacy Policy
Data Access Policies and Procedures
GLBA Policy
Data Retention and Archiving Policies and Procedures
Information Security Policies and Procedures
Rivier University FERPA Policy

State and Federal regulations

Related Policy
State of New Hampshire
The Family Educational Rights and Privacy Act of 1974
The Health Insurance Portability and Accountability Act of 1996
The Gramm Leach Bliley Act (GLBA)
The Fair and Accurate Credit Transaction Act of 2003 (FACTA or “Red Flags Rule”)
the Privacy Act of 1974
E-Government Act of 2002
Federal Information Security Management Act of 2002 (FISMA)

10. Contacts

Division/ Department	Position or Office	Contact Information
Information Technology	CIO	603-897-8630 / itsupport@rivier.edu