William Paterson University Policy
University Policy

SUBJECT:	University Policy	TITLE:	Institutional Data Governance Policy

CATEGORY: Check One	Board of Trustees ☐	University ☒	Functional ☐	School/Unit ☐

Responsible Executive:	President and Cabinet Members	Responsible Office:	Institutional Effectiveness, Information Technology, All Divisions/Cabinet

CODING:	00-01-	ADOPTED:		AMENDED:	

LAST REVIEWED: 07/10/26

I. PURPOSE

William Paterson University treats institutional data as a strategic asset. This policy establishes a campus-wide framework to manage, protect, and enable responsible use of institutional data to facilitate University operations and internal/external data reporting. It applies to all institutional data regardless of format, system, or medium, and to all members of the University community and third parties who use and access University data.

II. ACCOUNTABILITY

The Executive Data Oversight Committee (EDOC) provides strategic direction, sponsorship, and accountability for data domains under its oversight. EDOC approves policy, resolves cross-domain issues, ensures compliance, supports peer validation of externally reported institutional data, and promotes a data-informed culture. The Data Governance Council operationalizes this policy. Data Stewards, Data Custodians, and Data Users are accountable for fulfilling their respective governance responsibilities.

III. APPLICABILITY

This policy applies to all institutional data and to all University employees, students, contractors, affiliates, and third parties who access or use University data.

IV. DEFINITIONS

Governing Bodies and Data Workers
Executive Data Oversight Committee (EDOC): Cabinet-level body providing oversight and policy authority.
Data Governance Council: Cross-functional body responsible for operational data management, security, and policy compliance.
Data Steward: Functional expert responsible for data quality, definitions, metadata, and management.
Data Custodian: IT/system administrator responsible for technical controls and security.
Data User: Any individual accessing University data for business purposes.
Data Categories
Public: Information intentionally released to the public (e.g., published policies, public reports).
Internal: Business information intended for internal use that would pose minimal risk if disclosed (e.g., internal memos, non-public dashboards). It should be noted that the use of any William Paterson Power BI dashboards for external reporting is strictly prohibited.

Sensitive: Information protected by law, regulation, contract, or policy (e.g., FERPA-protected student records, employee data, as well as alumni and donor information).
Restricted: Highest-risk information requiring stringent controls (e.g., GLBA-regulated financial information, PCI cardholder data, HIPAA, etc. where applicable).

V. BACKGROUND

Institutional data is a shared University resource. The University supports appropriate access while protecting privacy and security, promotes data quality and transparency, supports data-informed decision-making and data literacy, and complies with applicable laws, regulations, contracts, and accreditation requirements.

VI. REFERENCES

William Paterson Policies Related to Data Use
Information Technology Policies
Generative AI Policy and Guidelines for Employees
AI: Use of Generative Artificial Intelligence in Student Academic Coursework
Cybersecurity Data Breach Procedure (forthcoming at this writing)

VII. POLICY

A. Requirements:

- Establish governance through EDOC and the Data Governance Council.
- Classify data as Public, Internal, Sensitive, or Restricted.
- Grant access based on business need, least privilege, and separation of duties.
- Maintain approved business definitions, metadata, and institutional reporting standards.
- Implement security, privacy, AI, predictive analytics, incident management, vendor management, training, and compliance requirements.

B. Responsibilities

- EDOC, Data Governance Council, Data Stewards, Data Custodians, and Data Users shall perform the responsibilities described in the policy.
- Data Stewards ensure data quality, definitions, validation, and issue resolution.
- Data Custodians implement technical controls, backups, recovery, and security.
- Data Users comply with policy and training requirements.

C. Enforcement:

Compliance may be assessed through audits and reviews. Violations may result in corrective actions and disciplinary measures. Information security and privacy incidents must be reported immediately.

VIII PROCEDURES

- Access requests require supervisor and Data Steward approval and are implemented by Enterprise Information Systems.
- Access reviews occur at least annually and upon role changes.
- External institutional reporting requires peer verification.
- Suspected incidents must be reported to Information Technology, supervisors, and Data Stewards.
- IT activates applicable breach-response or disaster-recovery procedures as needed.
- This policy will be reviewed at least every two years by the Data Governance Council and approved by the Data Oversight Committee

IX. EXHIBITS

Exhibit A – Governance Structure and Roles
Exhibit B – Descriptions of Relevant Data Governance Topics
- Predictive Analytics & Model Governance
- Third-Party Vendors & Data Sharing
- Academic Research Data Stewardship,
- Training & Awareness

Exhibit C –External References

Exhibit A – Governance Structure and Roles
Governance Structure
William Paterson uses a bicameral structure with executive oversight and operational governance:
Executive Data Oversight Committee (EDOC)

Cabinet members responsible for areas that use institutional data comprise the Executive Data Oversight Committee (EDOC), which provides strategic direction, sponsorship, and accountability for data domains under its oversight. They approve policy, resolve cross-domain issues, and support a data-informed culture. EDOC members are responsible for compliance as well as for ensuring peer validation of all institutional data that is sent out externally by employees in their divisions. The EDOC will also engage in cultivating a culture of data-driven decision making across their divisions. This Executive Data Oversight Committee will meet twice a year and as needed to resolve any cross-domain issues.

Data Governance Council

The Data Governance Council is a cross-functional body responsible for operationalizing this policy: defining data standards, approving institutional data definitions, maintaining the William Paterson Data Cookbook, coordinating access controls, resolving data issues, and aligning governance practices across divisions. Members are designated by the EDOC and meet regularly, at least quarterly.

Roles
- **Executive Data Oversight Committee member:** with policy authority for a data domain; designates Data Stewards and ensures compliance and serves on the Executive Data Oversight Committee.
- **Data Steward:** Functional expert responsible for the day-to-day management, quality, and definition of data within a domain; coordinates with IT on controls and access.
- **Data Custodian:** IT/system administrator responsible for technical controls, backups/recovery, performance, and security of systems storing institutional data.
- **Data User:** Any individual or system that accesses or uses data to conduct University business; must follow policy and training requirements.

Exhibit B – Descriptions of Relevant/Additional Data Governance Topics

Predictive Analytics & Model Governance
Predictive models used for University decision-making must be documented, approved for intended use, and monitored for performance, fairness, and drift. Predictive Analytics at William Paterson is primarily conducted in the areas of student success and retention, Finance, and other areas. For student success and retention, there is a Predictive Analytics Steering Committee, and its members will identify, select, and test models to be used in this area. Finance conducts predictive analytics internally. High-impact use cases require privacy and compliance review, human-in-the-loop oversight, and periodic audits. Third-party models must meet contractual, transparency, and security requirements.

Third-Party Vendors & Data Sharing
All external data sharing must be governed by appropriate agreements (e.g., Data Use Agreement, Business Associate Agreement for HIPAA, OPRA, GLBA/PCI contractual clauses). Vendors handling Sensitive or Restricted data must meet University security and privacy requirements, permit audit, and notify the University of incidents within contractually defined timeframes. The Office of General Counsel review of contracts includes checking for security terms.

Academic Research Data Stewardship
William Paterson University recognizes research data as a valuable institutional asset that supports scholarly inquiry, innovation, and public trust. The University is committed to responsible stewardship of research data throughout its lifecycle, and in accordance with legal, regulatory, contractual, and ethical obligations, and as informed by the Intellectual Property and Scholarly Works Agreement.

Training & Awareness
As new staff are onboarded, peer training on data classification, privacy, security, and appropriate data use is essential for Data Stewards, Custodians, and Users who access sensitive or restricted data. The culture of data literacy and data-informed decision-making should be strengthened at the university, which is the responsibility of members of the Executive Data Oversight Committee as they communicate with their divisions.

Exhibit C – External References
Brandeis University – Data Governance Policy: https://www.brandeis.edu/its/policies/data-governance-policy.html
Washington University in St. Louis – Data Governance Policy: https://data.wustl.edu/data-governance/data-governance-policies-2/- University of North Carolina – University Data Governance Policy: https://policies.unc.edu/TDClient/2833/Portal/KB/PrintArticle?ID=131263
EDUCAUSE – 2023 Horizon Action Plan: Data Governance: https://library.educause.edu/resources/2023/3/2023-educause-horizon-action-plan-data-governance
EDUCAUSE Review – Data Classification in Higher Education: https://er.educause.edu/articles/2025/2/policies-and-practices-how-to-improve-data-classification-in-higher-education
Columbia University – Data Classification Policy: https://universitypolicies.columbia.edu/content/data-classification-policy
ECU – GLBA Compliance in Higher Education: https://datagovernance.ecu.edu/gramm-leach-bliley-act-glba-compliance-at-ecu/
Thompson Coburn – Higher Ed GLBA FAQ (2025): https://www.thompsoncoburn.com/wp-content/uploads/2025/07/Higher-Ed-GLBA-FAQ-2025-Infosheet.pdf
University of California – Research Data Policy: https://osc.universityofcalifornia.edu/wp-content/uploads/2022/08/UC-Research-Data-Policy.pdf
NIH Scientific Data Sharing: Policies and Access to Data: https://sharing.nih.gov/

By Direction of the President and Cabinet:

Date: July 10, 2026

Chief Information Officer