

POLICY 3.2 – Data Governance Policy

POLICY SECTION:	Administrative – Information Technology
RELATED BOARD POLICY:	1.4.6 Records Management
RELEVANT LEGISLATION:	N/A
PRIMARY APPROVER:	President
SECONDARY APPROVER:	
RESPONSIBLE AUTHORITY:	Institutional Planning and Analysis Committee
DATE APPROVED:	
DATE(S) REVIEWED / REVISED:	
POLICY REVIEW - FREQUENCY:	To be reviewed every 3 years.
APPROVER SIGNATURE(S):	

1. Purpose

This Data Governance Policy establishes a framework for managing and protecting King's data assets. It defines roles, responsibilities, and structures to ensure the effective, ethical, and secure use of data in support of the King's mission, values, and strategic goals.

2. Scope of the Policy

This policy applies to all members of the King's University community, including faculty, staff, students, contractors, and any individuals or entities granted access to the University's data resources. It encompasses all data collected, stored, processed, or disseminated by King's, regardless of format or location.

3. Definitions

Data Governance: The practice of managing data as a strategic asset to ensure its quality, security, and usability.

Data Owner: An individual or entity accountable for the accuracy, integrity, and security of specific data assets. They have decision-making authority over the data and ensure its proper management.

Data Steward: An individual responsible for the oversight and management of specific data domains.

Data Custodian: A technical professional responsible for the safe storage, transport, and processing of data.

Data User: Any individual or group accessing and using University data for operational, educational, or research purposes.

Data Domains: Logical groupings of related data that are managed and governed collectively, such as student data, financial data, or research data.

Data Realm: Refers to a logical domain or boundary within an organization or system where data is governed, managed, and understood under a common set of rules, ownership, and purposes.

Institutional Data: All data owned or managed by the University, including academic, administrative, research, and operational data.

4. Governance Structure The governance structure ensures the proper management, use, and protection of institutional data. The following roles and bodies are established:

4.1 Institutional Planning & Analysis Committee (IPAC):

Purpose: Oversee data governance policies, standards, and practices.

Authority:

- Approve data governance policies and frameworks.
- Allocate resources for data management and governance.
- Resolve disputes related to data access and usage.

Responsibilities:

- Develop and maintain data governance policies and standards.
- Ensure compliance with regulatory and ethical standards.
- Provide strategic direction for data management.
- Review and endorse data quality and security measures.
- Ensure alignment of data governance with institutional goals.

4.2 Data Officer:

- **Role:** Executive sponsor and strategic leader for university-wide data and IT initiatives.
- **Responsibilities:**
 - Ensure alignment between IT infrastructure and data governance goals.
 - Provide resources for data governance implementation.
 - Collaborate and guide data owners and custodians to ensure data security and accessibility.

4.3 Data Owners:

- **Role:** Accountable for the data assets within their scope, ensuring data accuracy, integrity, and security.
- **Responsibilities:**
 - Make decisions regarding the use, access, and sharing of data.
 - Collaborate with data stewards and custodians to define and enforce data standards.
 - Ensure compliance with institutional policies and regulations.

4.4 Data Stewards:

- **Role:** Manage specific data domains, ensuring data accuracy, consistency, and compliance.
- **Responsibilities:**
 - Define data standards and quality requirements.
 - Monitor data usage within their domain.
 - Collaborate with data custodians to implement security measures.

4.5 Data Custodians:

- **Role:** Provide technical support for data storage, processing, and access.
- **Responsibilities:**
 - Implement technical controls to protect data integrity and confidentiality.
 - Support data access requests in accordance with university policies.
 - Maintain backup and recovery protocols.

4.6 Data Users:

- **Role:** Access and use data responsibly.
- **Responsibilities:**
 - Adhere to data governance policies and guidelines.
 - Protect data from unauthorized access, disclosure, or misuse.
 - Report data quality or security concerns.

5. Policy Guidelines

5.1 Data Classification: Data must be classified based on sensitivity and criticality, following the King's Data Classification Policy (e.g., public, sensitive, confidential).

5.2 Data Quality: All institutional data must be accurate, complete, timely, and relevant for its intended purpose.

5.3 Data Access and Usage: Access to institutional data is granted based on roles and responsibilities and governed by the rule of least privilege. Unauthorized access or misuse is strictly prohibited.

5.4 Data Security: Appropriate technical and administrative measures must be in place to protect data from threats such as breaches, loss, or corruption.

5.5 Regulatory Compliance: King’s will comply with all applicable laws, regulations, and ethical standards, including privacy and data protection laws.

6. Implementation and Enforcement

6.1 The Institutional Planning & Analysis Committee (IPAC) will oversee the implementation of this policy.

6.2 Violations of this policy will be addressed in accordance with university disciplinary procedures and applicable laws.

7. Review and Updates This policy will be reviewed triennially by the Institutional Planning & Analysis Committee and updated as needed to address emerging challenges, technologies, and regulatory changes.

8. Contact Information Questions or concerns regarding this policy should be directed to the Institutional Planning & Analysis Committee at IPAC@kings.uwo.ca.