POLICY 3.3 – Data Management 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 The purpose of this Data Management Policy is to establish standards and guidelines for ensuring the quality, sharing, integration, acceptable use, and retention of university data. This policy aims to enhance data integrity, promote responsible data use, and ensure compliance with legal, regulatory, and institutional requirements.

2. Scope This policy applies to all University personnel, including faculty, staff, students, contractors, and third-party service providers who create, access, process, or manage University data in any format or location.

3. Data Quality

3.1 Data Accuracy

- All institutional data must be accurate, complete, and up to date.
- Data Owners are responsible for defining data quality standards for their respective data domains.
- Periodic data audits and validation checks will be conducted to ensure data accuracy.

3.2 Data Consistency

- Data must be consistent across different systems and reports.
- Standardized data formats, nomenclature, and definitions shall be used across the University.

3.3 Data Timeliness

- Data should be captured and updated in a timely manner to support decision-making.
- Outdated or redundant data must be flagged for review and removal.

4. Data Sharing

4.1 Internal Data Sharing

- Data may be shared across departments or data realms for operational and strategic purposes based on access controls and need-to-know principles.
- Requests for internal data sharing must be approved by the relevant Data Owner.

4.2 External Data Sharing

- Data sharing with external parties must comply with university policies, data classification guidelines, and applicable legal and regulatory requirements.
- Data sharing agreements must be established for any third-party data access.

4.3 Data Sharing Security Measures

- Secure channels and encryption must be used for data transfers.
- Access to shared data must be reviewed periodically.

5. Third-Party Data Use

5.1 Vendor Management

- Third-party vendors handling University data must comply with data security and privacy requirements.
- Service-level agreements (SLAs) must specify data protection obligations.

5.2 Compliance and Monitoring

- Third-party data handling practices shall be regularly assessed to ensure compliance with university standards.
- Non-compliance by vendors may result in contract termination and legal action.

6. Data Integration

6.1 Data Consolidation

- University systems should support integration efforts to maintain a single source of truth for key institutional data.
- Data integration must follow established data governance and security protocols.

6.2 System Interoperability

- Systems used for data integration should adhere to interoperability standards and support seamless data exchange.
- Data integration efforts must minimize duplication and inconsistencies.

7. Acceptable Data Use

7.1 Data Use Principles

- University data must be used ethically, legally, and in alignment with the institution's values.
- Users must follow University data governance policies and ethical guidelines.

7.2 Prohibited Data Use

- Misuse of data, including unauthorized access, distribution, or modification, is strictly prohibited.
- Violations of acceptable data use policies may result in disciplinary actions.

7.3 User Responsibilities

- All users are responsible for maintaining data confidentiality, integrity, and availability.
- Data Users must report any data misuse or security incidents.

8. Data Retention and Disposal

8.1 Data Retention Periods

- Data shall be retained in accordance with regulatory, legal, and operational requirements.
- Data Owners are responsible for establishing and enforcing retention schedules.

8.2 Secure Disposal Methods

- Data no longer required must be securely disposed of following University guidelines.
- Methods of disposal include shredding, deletion, and degaussing of electronic media.

8.3 Data Archiving

- Data deemed historically significant may be archived in accordance with institutional archiving policies.
- Archived data must remain protected from unauthorized access.

9. Compliance and Enforcement

- Compliance with this policy is mandatory, and violations may result in disciplinary action up to and including termination.
- The Institutional Planning & Analysis Committee (IPAC) will oversee policy enforcement and provide guidance.

10. Review and Updates This policy will be reviewed triennially by the Institutional Planning & Analysis Committee to ensure its continued relevance and effectiveness.

11. Contact Information For questions or concerns regarding this policy, please contact the Institutional Planning & Analysis Committee at IPAC@kings.uwo.ca.