POLICY 3.7 – Data Compliance and Risk 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 Compliance and Risk Management Policy is to ensure that the University's data assets are managed in compliance with legal, regulatory, and institutional requirements. This policy aims to identify, assess, and mitigate risks associated with data handling and establish a culture of compliance and accountability.

2. Scope This policy applies to all King's 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 Compliance

3.1 Regulatory Compliance

- The University shall comply with all applicable data protection laws and regulations, including but not limited to FIPPA, and PHIPA,.
- All departments must align their data management practices with these regulations.
- Regular compliance audits will be conducted to ensure adherence to legal and regulatory frameworks.

3.2 Institutional Policies and Guidelines

- Compliance with internal data governance policies, including Data Classification, Data Privacy, and Data Security policies, is mandatory.

- Data Owners are responsible for enforcing compliance within their respective data domains.

3.3 Training and Awareness

- All personnel must complete mandatory data compliance training.
- Ongoing education and awareness programs will be conducted to ensure understanding of compliance requirements.

4. Risk Management

4.1 Risk Identification

- Data risk assessments shall be conducted periodically to identify potential vulnerabilities.
- Risks will be categorized based on their impact and likelihood, with priority given to high-risk areas.

4.2 Risk Assessment and Mitigation

- The University shall implement a structured risk assessment process to evaluate and mitigate identified risks.
- Risk mitigation plans shall include preventive, detective, and corrective measures.
- Risk acceptance and exceptions must be approved by the Institutional Planning & Analysis Committee (IPAC).

4.3 Incident Reporting and Response

- All data-related incidents must be reported immediately to the IT Security Team and/or the Privacy Officer.
- The IT Security Team and/or the Privacy officer will inform the appropriate data owner.
- The University's Incident Response Plan shall be followed to contain and address risks effectively.
- A post-incident review will be conducted to identify root causes and improve processes.

5. Roles and Responsibilities

5.1 Institutional Planning & Analysis Committee (IPAC)

- Provide oversight and strategic direction for data compliance and risk management.
- Approve risk management frameworks and compliance programs.

5.2 Data Officer

- Ensure implementation of compliance controls and risk management strategies.

- Allocate resources for compliance initiatives and risk mitigation.

5.3 Data Owners

- Ensure compliance with regulatory and institutional policies within their domains.
- Identify and report potential risks to IPAC.

5.4 Data Stewards

- Monitor compliance and assist in risk assessments within their data domains.
- Implement corrective actions as needed.

5.5 Data Custodians

- Maintain security controls to mitigate risks and ensure compliance.
- Provide audit logs and reports for review.

5.6 Data Users

- Adhere to compliance requirements and report any potential risks or incidents.
- Participate in required compliance training.

6. Compliance Audits and Reporting

- Regular audits will be conducted to evaluate compliance with this policy.
- Non-compliance will be addressed through corrective actions, remedial training and may result in disciplinary measures.
- Audit results and risk assessments will be reported to IPAC for review.

7. Review and Updates This policy will be reviewed triennially by the Institutional Planning & Analysis Committee to ensure its continued relevance and effectiveness in mitigating data risks.

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