Information Governance Policy

1. Purpose

1.1 This policy sets out Bath Spa University's commitment to managing information lawfully, securely and effectively. It establishes a unified framework that integrates five interdependent domains: data protection, access to information, records management, information security and business continuity into a single system of governance and accountability. This system ensures that all information assets are handled in a way that supports legal compliance, operational resilience and public trust.

2. Scope

2.1 The Policy applies to all employees, contractors, volunteers and third-party service providers who create, access, process or manage information on behalf of the University. It covers all formats of information, including electronic, printed, audio, visual and all categories including personal data, commercial and confidential business information and public records.

2.2 Implementation is supported by an Information Governance Programme that continuously develops the resources, processes and technologies to embed mature information governance practices across the organisation and it is also aligned with the Business Continuity Strategy.

3. Integrated Domains of Governance

3.1 The governance model is designed to ensure cross-domain oversight and accountability, covering the following domains:

Data Protection
Personal data is processed lawfully, fairly and transparently in accordance with UK GDPR. Privacy by Design is embedded into all systems and processes. Data minimisation, purpose limitation and individual rights are upheld through documented procedures and regular audits.

Access to Information
The University complies with the Freedom of Information Act 2000 and supports Subject Access Requests under UK GDPR. Procedures are in place to ensure timely, accurate and lawful disclosure of information, balancing transparency with confidentiality and security obligations.

Records Management
Information is managed throughout its lifecycle – from creation and classification to retention and secure disposal. The University maintains a Records Retention Schedule aligned with legal and operational requirements. Metadata standards and audit trails ensure traceability and accountability. The Records Retention Schedule is aligned with JISC's Business Classification Scheme and Records Retention Schedule to ensure sector-wide consistency.

Information Security
Technical and organisational controls are in place to protect the confidentiality, integrity, availability and resilience of information. These include access controls, encryption, threat monitoring and incident response protocols. Security measures are proportionate to the sensitivity and criticality of the information.

Business Continuity
Information assets and systems are protected against disruption through documented continuity plans, backup procedures and recovery testing. Critical records and services are prioritised to ensure resilience and rapid restoration in the event of an incident.

3.2 These domains are interlinked through shared governance roles, aligned policies and integrated operational controls. The University uses tools such as the ICO Accountability Tracker to monitor compliance across all domains, identify gaps and drive continuous improvement. This unified approach enables the University to demonstrate accountability to regulators, students and the public.

4. Policy Statement

4.1 BSU recognises that effective information governance is essential to maintain legal compliance, operational integrity and public trust and is committed to:

- Ensuring confidentiality, integrity and availability of information assets
- Complying with the Data (Use and Access) Act, UK General Data Protection Regulation, Data Protection Act 2018, Freedom of Information Act 2000 and sector-specific codes
- Embedding Privacy by Design and Default into all systems and processes
- Assigning Data Domain Owners, Data Owners and Data Stewards to ensure accountability and oversight of data
- Maintaining resilient IT services capable of withstanding scrutiny and attack
- Implementing business continuity and disaster recovery capabilities to enable information to be managed and accessed
- Participating in recognised certification schemes e.g. Cyber Essentials Plus
- Promoting a culture of transparency, accountability and continuous improvement
- Building trust with students, staff, educational partners, research partners and external stakeholders

4.2 Through taking this approach, the University affirms its commitment to a unified, accountable information governance system that ensures information is protected, accessible, well-managed and resilient across its entire lifecycle.

5. Governance and Accountability

5.1 The Board of Governors is responsible for overseeing the conduct of the affairs of the University and for safeguarding its assets (including information

assets). The Audit and Risk Assurance Committee of the Board of Governors is responsible for approval and oversight of this Information Governance Policy.

5.2 The Information Governance Group is responsible for overseeing the implementation of improvements identified to support the Information Governance Policy through the Information Governance Programme and for informing Senior Management and line managers of gaps that they need to address. The Business Resilience Group is responsible for the University's strategy and planning in respect of emergency management and business continuity.

5.3 The following roles have dedicated responsibilities with regards to this Policy:

Role	**Responsibility**
University Secretary	Strategic oversight of information risk with responsibility for the establishment and operation of the Information Governance Group and associated programme. Chair of the Business Resilience Group.
Information Governance Lead and Data Protection Officer	Advice and guidance on data protection obligations and IG Compliance.
Freedom of Information Officer	Freedom of Information Act compliance and request handling.
Chief Information Officer (CIO)	Digital transformation and IT strategy
Chief Technology Officer (CTO)	Technical infrastructure and innovation strategy, supporting digital transformation and IT operations. Member of the Business Resilience Group.
Chief Information Security Officer (CISO)	Information security strategy, regulatory compliance and cybersecurity resilience. Member of the Business Resilience Group.
Director of Data and Insights	Data-driven decision-making, analytics and institutional insights.
Senior management, Heads of Schools/Departments and line managers	Accountable and responsible for ensuring that the policy is understood, effectively applied and adhered to at all times.
All Staff	Familiarisation with this policy and complying with the requirements.

6. Operational Controls

6.1 BSU implements a range of operational controls to embed information governance principles into daily practice. These controls are designed to ensure compliance, mitigate risk and support continuous improvement across all departments and systems:

- Mandatory information governance related training for all staff, with annual refreshers and additional modules for specialist roles and those handling high-risk data
- Regular policy reviews and updates
- Breach and incident reporting procedures
- Internal audits and assurance checks
- Information governance requirements embedded in third-party contracts and data-sharing agreements
- Asset-level controls via Data Owners and Data Stewards
- Data Protection Impact Assessments (DPIA) for new systems and processes
- Privacy notices and consent mechanisms
- IT resilience testing and reporting
- Business continuity and disaster recovery plans tested regularly
- Open-data readiness and ethical data handling
- Staff must use approved platforms (e.g., SharePoint, Teams) for collaborative work involving personal or sensitive data. Email should not be used for long-term storage or sharing of such information
- A structured incident response framework is maintained to ensure timely escalation, containment and reporting of breaches. All incidents must be report to the DPO within 24 hours and assessed for regulatory reporting obligations.

6.2 These controls are monitored through regular reporting and assurance activities, with findings used to information strategic improvements and risk mitigation.

7. Compliance and Assurance

7.1 To demonstrate accountability and meet regulatory expectations, BSU maintains robust documentation and assurance mechanisms. These provide evidence of compliance and support internal and external audits:

- Records of Processing (RoPA) maintained and reviewed
- DPIAs completed and logged
- Data Subject Access Requests (DSAR or SAR) and Freedom of Information requests tracked and responded to
- Retention schedules and disposal logs maintained
- ICO Accountability Framework used to assess compliance
- Certification submissions completed
- IT Service Register maintained and reviewed
- Business continuity testing results and recovery metrics reviewed regularly
- Risk assessments conducted and escalated

7.2 These assurance mechanisms are subject to oversight by the Information Governance Group and will form part of the annual compliance review cycle.

8. Monitoring and Review

8.1 This Policy is reviewed in accordance with policy review requirements and/or in response to significant changes in legislation, risk profile or organisational structure. Compliance is monitored through the Information Governance Group.

9. Breach and Non-Compliance

9.1 Non-compliance may result in disciplinary action and regulatory penalties. All breaches must be reported immediately and investigated per BSU procedures. BSU will maintain breach logs and report incidents to the Commission where required.

Document Details

Responsible Office: Governance, Legal & Compliance

Responsible Officer: University Secretary

Approving Authority: Audit and Risk Assurance Committee

Date of latest approval: 6 November 2025

Effective Date: 6 November 2025

Related Policies and Procedures:

Data Protection Policy 2025

Freedom of Information

Records Management Policy

Records Retention Policy and Retention Schedule

Research Data Policy

Supersedes: Information Governance Policy
18 December 2017

Next review due: 6 November 2030