Information Security Policy

1. Introduction

1.1 The digital ecosystem has evolved dramatically in recent years. Bath Spa University (BSU) has embarked on a remarkable journey of digital transformation, which also inevitably brings about challenges in the areas of security and privacy, compliance with new legislation and meeting the increased level of expectation of BSU's security posture by its partners, collaborators, auditors and customers. At the same time, the University is mindful of the need to strike the optimal balance between useability and security for its students and staff.

1.2 As a leading higher education institution committed to innovation and high-quality teaching, BSU has the ethical, legal and professional duty to ensure the information it holds conforms to the principles of confidentiality, integrity and availability. BSU is committed to ensure that the information it is responsible for is safeguarded where necessary against inappropriate or unauthorised disclosure; is accurate and attributable; and is available to those who should be able to access it.

1.3 The Information Security Policy provides the framework by which BSU meets those principles and duties. It is the cornerstone of BSU's continuous efforts to enhance its information security posture and cyber resilience.

2. Purpose

2.1 The primary purposes of this policy are to:

- Outline BSU's approach to Information Security Management;
- Provide the guiding principles to safeguard BSU's systems and information assets, preserving their confidentiality, integrity and availability;
- Ensure BSU meets its ethical obligations and legal duties under the information security and data protection regulations;
- Ensure members of the BSU community are aware of and comply with BSU's guiding information security principles;
- Ensure BSU's supply chain is managed securely, reducing the likelihood of compromise through a supply chain attack;
- Demonstrate BSU's commitment to meet expectations by its customers, the regulators, auditors, partners and collaborators.

3. Scope

3.1 This Policy is intended for all BSU staff, students, collaborators and third parties who interact with BSU systems and data. It applies to all BSU systems including Cloud systems, systems attached to BSU's telephone networks and devices that are connected to BSU networks or hold/access BSU data.

4. Policy

4.1 **Overarching principles**

The following principles provide overarching governance for BSU's information security practices.

4.1.1 Information should be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with BSU's Information Classification Scheme, relevant legislative, regulatory and contractual requirements.

4.1.2 Data owners shall establish the classification of information.

4.1.3 All users that are covered by the scope of this policy must handle information appropriately and responsibly, and in accordance with its classification level.

4.1.4 Information should be both secure and available to those who have a legitimate need for access.

4.1.5 Access to information must be based on 'least privilege' and 'need to know'.

4.1.6 Appropriate, proportionate, technical and organisational measures must be established to safeguard the information and enhance BSU's cyber resilience.

4.1.7 Breaches of this policy must be reported to IT Services where possible.

4.1.8 This policy is supported and underpinned by a series of technical guidance documents which describe the processes and activities undertaken by IT Services in the management of the University's technical infrastructure.

4.1.9 The Policy shall be reviewed annually.

4.1.10 Contractual security requirements imposed on BSU, if more stringent than those outlined in this policy, take precedence over this policy.

4.2. **Legal and Regulatory Obligations**

4.2.1 BSU has a responsibility to abide by all current and prospective UK legislation that are relevant to this policy.

4.2.2 Where appropriate BSU is obliged to adhere to a variety of regulatory and contractual requirements, for example the PCI DSS (Payment Card Industry Data Security Standards).

4.2.3 Appendix 1 provides a non-exhaustive list of applicable legislative and regulatory obligations.

4.3. Suppliers

4.3.1 BSU's suppliers, including their sub-contractors, while accessing BSU's systems and assets, whether on site or remotely, shall abide by BSU's Information Security Policy, or otherwise be able to demonstrate equivalent levels of assurance.

4.4 Cloud Application Providers

4.4.1 Where Cloud applications are commissioned, BSU remains as the data controller and has the obligation to report to the UK Information Commissioner's Office (ICO) should there be a data breach associated with such Cloud applications. With the proliferation of supply chain attacks, BSU is subject to risk of compromise through a third-party compromise in the supply chain.

4.4.2 Adequate security and data protection assessment must be carried out prior to commissioning Cloud applications, in accordance with the Third-party Applications Security Procedure, including:

- The Department intending to deploy applications or software shall inform IT Services prior to engagement with the supplies.
- Introduction of new applications must not contradict BSU's Architecture Principles.
- Where applicable a Data Protection Risk Evaluation (DPRE) and/or Data Protection Impact Assessment (DPIA) must be completed by the Department and reviewed by BSU's Information Governance team.
- Security assessment and DPIA must be signed off by the CISO and DPO respectively prior to acquisition. Where applicable the security assessment must be embedded in the tender process.
- The supplier's security posture shall be regularly re-visited preferably on an annual basis.

4.5. Incident handling

4.5.1 Anyone to whom this Policy applies must report to IT Services should a suspected information security incident come to their attention.

4.5.2 BSU's DPO (Data Protection Officer) will report breaches of personal data to the ICO and advise on further legal steps to attend to.

4.6 **Risk management**

4.6.1 Risks associated with cyber security must be recorded in IT Services' departmental risk register, and where appropriate feed up to the University's strategic risk register.

4.6.2 BSU's senior management shall have visibility of the University's cyber risk posture.

4.6.3 Risks deemed unacceptable but which cannot be treated must be recorded and escalated to the University's senior management as appropriate.

4.7. **Artificial intelligence (AI)**

4.7.1 AI systems often rely on large amounts of personal data. BSU has the ethical responsibility to ensure a proportionate level of assessment is carried out prior to commissioning AI systems.

4.8. **Compliance**

4.8.1 Any compromise of BSU's systems and data could lead to possible financial fines, costs associated with recovery activities, reputation loss, and in extreme scenarios, legal actions against BSU. As such it is crucial that all in-scope users adhere to this policy.

4.8.2 Any deliberate, malicious, intrusion to BSU's systems by BSU members could result in disciplinary procedures.

5. Responsibilities

Members of BSU

All users identified in the scope of this Policy have the responsibility to adhere to this policy and relevant legislation, supporting policies, procedures and guidelines. This includes the responsibility to report a suspected security incident should it come to their attention.

Collaborators and third parties

Collaborators and third parties who interact with BSU systems and data are obliged to adhere to this policy.

Data Owners and Data Custodians

Data owners and custodians have the responsibility where applicable for preserving the confidentiality, integrity and availability of information.

Senior Information Risk Officer (SIRO)

BSU's School Secretary acts as the SIRO and is accountable for BSU's compliance with information security and data protection regulations.

Information Governance Group (IGG)

BSU's IGG is responsible for information governance oversight. The approval of new policies is owned by the Senior Leadership Group (SLG).

IT Services

IT Services acts as the initial point of contact where a security incident occurs and is responsible for collaborating with relevant internal and external stakeholders to carry out the incident response.

Data Protection Officer (DPO)

The DPO is responsible for reporting the data breach to the ICO and advise on further legal steps as appropriate.

Appendix 1 - Summary of relevant legislation

The Computer Misuse Act 2024

Defines offences in relation to the misuse of computers as:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised acts with intent to impair, or with reckless as to impairing, operation of computer, etc.
- Unauthorised acts causing, or creating risk of, serious damage
- Making, supplying or obtaining articles for use in offence

Data Protection Act 2018 and UK GDPR

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). It controls how personal information is used by organisations, businesses, or the government.

The Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA2000) is a general right of public access to all types of recorded information held by public authorities to promote a culture of openness and accountability.

General Data Protection Regulation and DPA 2018

The GDPR has applied to the UK since 25 May 2018. The GDPR reinforces and extends data subjects' rights as laid out in the Data Protection Act (1998), and provides additional stipulations around accountability and governance, breach notifications and transfer of data. It also extends the maximum penalties liable due to a data breach, from £500,000 to up to 4% global turnover.

The GDPR places many obligations on BSU including having Records of Processing, ensuring that where personal data is voluntarily gathered, individuals explicitly opt in and can also easily opt out. It requires certain breaches to be reported to the Information Commissioner's Office within 72 hours of BSU becoming aware of their existence.

Digital Information and Smart Data Bill

Introduced in the King's speech, it is intended to replace the Data Protection and Digital Information Bill which was progressing through Parliament.

PCI DSS (Payment Card Industry Data Security Standards)

PCI DSS is a set of mandatory industry security standard where merchants taking card payments must adhere to. The level of compliance differs depending on the merchant's volume of transactions.

Investigatory Powers Act 2024

This Act regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

Online Safety Act 2023

Regulates online speech and media with the aim of protecting children and adults online. Providers have the duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear.

Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008

Section 160 of the Criminal Justice Act 1988 made the simple possession of indecent photographs of children an offence. Making an indecent image of a child is a serious arrestable offence carrying a maximum sentence of 10 years imprisonment. Note: The term "make" includes downloading images from the Internet and storing or printing them out.

Section 63 of the Criminal Justice and Immigration Act 2008 made it an offence being in possession of an extreme pornographic image.

Defamation Act 2013

Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm.

Obscene Publications Act 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

Terrorism Act 2006

- The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.
- It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.
- In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such

offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.

Counter-Terrorism and Security Act 2015 and its Statutory Guidance

Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on specified authorities – including most higher education institutions – to have 'due regard to the need to prevent people from being drawn into terrorism'. This is commonly referred to as the 'Prevent duty'.

The statutory guidance accompanying the Counter-Terrorism and Security Act 2015 requires BSU to have “due regard to the need to prevent people from being drawn into terrorism.” The Act imposes certain duties under the Prevent programme, which is aimed at responding to “the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views.” The Prevent programme also aims to provide “practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support”. BSU must balance its existing legal commitments to uphold academic freedom and (under the Education (No. 2) Act 1986) freedom of speech within the law against the new Prevent duty and seek to ensure that its IT facilities are not used to draw people into terrorism.

Document Details

Responsible Office: IT Services

Responsible Officer: Chief Information Officer

Approving Authority: Senior Leadership Group

Date of latest approval: November 2024

Effective Date: November 2024

Related Policies and Procedures: Information Classification Scheme, Data Protection Policy, Records Management Policy, AI Policy

Supersedes: N/A

Next review due: September 2025