# University of Bristol

# Information Security Policy - Compliance

| | |
|---|---|
| **Title** | Compliance |
| **Reference** | ISP-03 |
| **Status** | Approved |
| **Version** | 3.0 |
| **Date created** | December 2012 |
| **Last reviewed** | January 2024 |
| **Next review** | January 2025 |
| **Classification** | Public |

## Contents



## 1. Introduction

This Compliance Policy is a sub-policy of the Information Security Policy (ISP-01) and outlines the University's requirement to comply with certain legal and regulatory frameworks. This policy is to be read in conjunction with the University's Guide to Information Legislation, which provides details of the legislation relevant to information security, for example the Data Protection Act.

## 2. Scope

All members of the University (as defined in the University's Constitution: Ordinance 9, Section 7), members of other institutions who have been granted federated access to use the University's facilities, and any others who may have been granted permission to use the University's information and communication technology facilities by the Chief Digital and Information Officer are subject to this policy.

## 3. Policy

### 3.1 Compliance with the University's Information Security Policy

The University's own information security policies must be adhered to whenever an individual or organisation is handling University information. The University must ensure it is acting legally when following such policies.

All staff, students and other persons who may handle University information must be made aware of the University's information security policies and of any amendments made to them. Individuals must also confirm that they have read and understood these policies and how they apply to the information they handle.

### 3.2 Compliance with Legislation

The University requires its members to comply with relevant legislation to help prevent breaches of the University's legal obligations. However, individuals are ultimately responsible for ensuring that they do not breach legal requirements during the course of their work or studies.

The University must comply with all relevant legal requirements whether such requirements are detailed in internal policies or not. Any suspected breach of the University's legal requirements must be reported to the Legal Services and Secretariat.

The Guide to Information Legislation document gives further details of the relevant legal requirements the University must adhere to.

Users of the University's online or network services are individually responsible for their activity and must be aware of the relevant legal requirements when using such services.

Other regulatory requirements are set out below.

### 3.3 Statutory Information Access Requests

Under UK Freedom of Information and Data Protection legislation, individuals as well as agencies with statutory powers are entitled to request recorded information and personal data from the University.

When processing statutory information access requests, the University is subject to the requirements of the above legislation, which includes the provision of access to, and disclosure of, certain information.

### 3.4 Collection of Evidence

At times, it may be necessary for the University to collect evidence in relation to a potential legal claim or internal investigation.

Where there is suspicion of a criminal offence involving the University's information or systems, the University will cooperate with the relevant agency to assist in the preservation and gathering of evidence on the basis of appropriate internal authorisation and compliance with relevant statutory requirements.

Please refer to the University's Investigation of Computer Use Policy (ISP-18) for additional guidance.

### 3.5 Records Management

The University is required to retain certain information, whether held in hard copy or electronically, for legally defined periods. Such information must be appropriately safeguarded and not destroyed prior to the defined minimum retention period, while remaining accessible to those who require access and are authorised to access that information.

In accordance with the UK Data Protection legislation, personal data should not be retained for longer than it is required for the purposes for which it was collected.

For additional guidance refer to the University's Records Retention Schedule and the Records Management and Retention Policy.

### 3.6 Payment Card Industry Data Security Standard (PCI DSS)

The University must comply with the Payment Card Industry Data Security Standard (PCI DSS) and the relevant legislation when processing payment (credit/debit) cards. To assist with this compliance, the University has published its own PCI DSS Cardholder Data Policy (ISP-19).

### 3.7 Software License Management

All software used for University business must be appropriately licensed. The University must comply with the software and data licensing agreements it has entered into. During the negotiation process of such agreements, full consideration must be given to how compliance with the agreement can practically be achieved. Agreements may need to be specifically negotiated to enable the University to comply.

Please refer to the University's Software Management Policy (ISP-13) for additional guidance.

### 3.8 JANET Policies

The University, along with other UK educational and research institutions, uses the 'JANET' (Joint Academic NETwork) electronic communications network and must therefore comply with JANET's Acceptable Use and Security Policies. These policies are available on the JANET Website (https://community.jisc.ac.uk/library/janet-policies).

## 4. Further Guidance

- Legal Services and Secretariat website:
  https://www.bristol.ac.uk/secretary/
- University's Guide to Information Legislation:
  https://www.bristol.ac.uk/media-library/sites/infosec/documents/guide.pdf
- ISP-18 Investigation of Computer Use:
  https://www.bristol.ac.uk/infosec/policies/investigation-of-computer-use-policy/
- Records Retention Schedule:

https://www.bristol.ac.uk/media-library/sites/secretary/documents/information-governance/records-retention-schedule-v1.1.pdf

- Records Management and Retention Policy: https://www.bristol.ac.uk/media-library/sites/secretary/documents/information-governance/records-mangement-and-retention-policy-v1.1.pdf

- ISP-19 PCI-DSS Cardholder Data: https://www.bristol.ac.uk/infosec/policies/payment-card-industrys-data-security-standard-pci-dss-cardholder-data-policy/

- ISP-13 Software Management: https://www.bristol.ac.uk/infosec/policies/software-management-policy/

- ISP-04 Outsourcing and Third Party Compliance: https://www.bristol.ac.uk/infosec/policies/outsourcing-and-third-party-compliance-policy/

- JANET acceptable Use and Security Policies: https://community.jisc.ac.uk/library/janet-policies