Compliance Policy (ISP-03)

1. Introduction
2. Scope
3. Policy
    - 3.1 Compliance with the University Information Security Policy
    - 3.2 Compliance with Legislation
    - 3.3 Statutory Information Access Requests
    - 3.4 Collection of Evidence
    - 3.5 Records Management
    - 3.6 Payment Card Industry Data Security Standard (PCIDSS)
    - 3.7 Software License Management
    - 3.8 Third Party Terms and Conditions
    - 3.9 JANET Policies
4. Further guidance

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

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 UK GDPR.

3. Policy

3.1 Compliance with the University Information Security Policy

The University own Information Security Policies must be adhered to at 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 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 in the following subsections.

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 please 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 Licence 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 Software Management Policy (ISP-13) for additional guidance.

3.8 Third Party Terms and Conditions

Where the University uses the services of a third party provider, members of the University will also be subject to their terms and conditions in so far as they relate to information security.

Please refer to the University Outsourcing and Third Party Compliance Policy (ISP-04) for additional guidance.

3.9 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
- University's Guide to Information Legislation
- Investigation of Computer Use Policy (ISP-18)
- PCI DSS Cardholder Data Policy (ISP-19)
- University's Records Retention Schedule
- University's Records Management and Retention Policy
- Software Management Policy (ISP-13)
- Outsourcing and Third Party Compliance Policy (ISP-04)
- JANET Acceptable Use and Security Policies

Title	Compliance Policy
Reference	ISP-03
Status	Approved
Version	4.0
Date Created	March 2014
Last Reviewed	December 2024

Next Review	December 2025
Classification	Public
PDF Policy Link	Compliance Policy - ISP-03 (PDF, 174kB)