University of Bristol
Information Security Policy

Title:	**Compliance Policy**
Reference:	**ISP-03**
Status:	**Approved**
Version:	**1.2**
Date:	**December 2012**
Reviewed:	**August 2019**
Classification:	**Public**

Contents

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 e.g. the Data Protection Act.

Compliance with legislation

The University provides policy statements and guidance for staff and students in relation to compliance 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.

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.

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 Registrar.

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

Other regulatory requirements are set out below.

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. Both of these policies are available from the JANET Website (https://community.jisc.ac.uk/library/janet-policies).

Payment Card Industry Data Security Standard (PCI DSS)

The University must comply with the Payment Card Industry Data Security Standard (PCI DSS) and the re when processing payment (credit/debit) cards. To assist with this compliance, the University has published its own PCI DSS policy available on the Information Security section of its website (http://www.bristol.ac.uk/media-library/sites/infosec/documents/IPS%20-19.pdf)

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.

Third party terms and conditions

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

Compliance with the University's Information Security Policy

The University's own information security policies must be adhered to at all times when handling University information and the University must ensure it is acting legally when operating 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.

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.

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 Data Protection Act, personal data should not be retained for longer than it is required for the purposes for which it was collected.

Further information can be found on the University Secretary's Office website (http://www.bristol.ac.uk/secretary/information-governance/)