Keele University Information Security Policy

Owner	Director of Finance & IT		
Approver	Council	**Date**	4 May 2017
Version Number	Version 1.0	**Version date**	4 May 2017
Implementation:	This Code of Practice will be implemented directly after its implementation date.		

Printed versions of this document are uncontrolled and only valid for 14 days and may be subject to amendment at any time.

The latest version of this Policy can be found at https://www.keele.ac.uk/policyzone/
Any superseded versions of this document need to be promptly withdrawn from use.

Approval and Amendment History v1.1 Approved by	
Lead	Director of Finance & IT
Review Period	Every two years
Date of next review	May 2019

Keele University Information Security Policy

1. Introduction

Keele University is reliant on its information assets to function effectively. It is essential that the University's information assets are protected against the consequences of breaches of confidentiality, failures of integrity and interruptions to availability. An information security breach could damage the University's reputation, cause distress to individuals, and result in a substantial fine (currently up to £500,000) from the Information Commissioner's Office.

2. Background

The University has an Information Security Management System which provides a framework for the protection of the University's information assets. This policy forms part of this system.

The Information Security Management System is based on the requirements stated within the ISO27001 Information Security Management System international standard and the University and Colleges Information Systems Association (UCISA) Information Security Management Toolkit. This policy is supported by the other guidance, processes and procedures that form part of the University's Information Security Management System.

3. Objectives

3.1 The primary objectives of this Policy are to:

- ensure the protection of all the University's information assets and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these assets;
- ensure that the University implements good practice in accordance with the ISO27000 series information security standards, the UCISA Information Security Management Toolkit, NHS Information Governance Toolkit and the Payment Card Data Security Standard;
- ensure that the University's authorised users are aware of and are in a position to comply with all current and relevant UK and EU legislation;
- ensure that the University's authorised users understand and comply with this policy and the other associated policies and guidance documents;
- ensure that the University's authorised users understand their own responsibilities for protecting, preserving and managing the confidentiality, integrity and availability of the University's information assets; and
- ensure that the University is protected from the potential consequences of security breaches.

4. Scope

This policy applies to anyone with access to the University's information assets including staff, students, visitors and contractors. Information assets include but are not limited to all computers, mobile devices, networking equipment, systems, databases, data files, hard copy documentation, visual media and software.

5. Information Security Principles

5.1 All the University's information assets whether electronic or in hard-copy form must be protected against unauthorised access.

5.2 The University's information assets must be available to all those who have a legitimate need to access them.

5.3 The integrity of the University's information must be maintained so that it is accurate and complete.

5.4 All users of the University's information systems will comply with the University's information security and data protection policies and guidance including the IT Conditions of Use. It is the responsibility of users to ensure that they continually familiarise themselves with and fully understand the contents of the policies and guidance. Failure to comply with the information security policies and guidance may result in disciplinary action.

5.5 All users of the University's information systems will abide by and adhere to all current UK and EU legislation as well as regulatory and contractual requirements. See Appendix A for a list of the relevant requirements (which may be updated from time to time).

5.6 All the University's information assets will be inventoried.

5.7 All information assets will be classified according to their required levels of confidentiality. The classification of the asset will determine the security controls that will be applied to it and how it must be handled.

5.8 All information assets will be assigned an owner who will be responsible for ensuring that the asset has the correct information classification, has adequate protection and is handled at all times in accordance with its classification.

5.9 Key information assets will be subject to annual risk assessments to identify the probability and impact of security failures. The results of the risk assessments will determine the appropriate security controls to be applied to the assets.

5.10 All users of Keele information systems shall receive information security training appropriate to their role and to the classification of information assets they have access to.

5.11 All suspected and actual information security breaches must be recorded and reported to the IT Service Desk who will then refer any significant breaches to the Deputy Director of Finance & IT and the Information Security Manager.

5.12 All departments will produce Disaster Action Plans for their critical systems. The Disaster Action Plans must be reviewed and periodically tested against.

6. Information Security Responsibilities

6.1 Vice Chancellor and the University Executive Committee

The Vice Chancellor has the ultimate responsibility for information security at the University. The Vice Chancellor supported by the University Executive Committee will ensure that the University complies with relevant external requirements including legislation and contractual obligations. The Vice Chancellor and the University Executive Committee are responsible for the overall direction and commitment to information security. The Committee will approve information security policies and guidance, provide high level support for security initiatives and review the adequacy of the University's Information Security Management System. Deans and Directors will take responsibility for operational compliance within their areas of responsibility.

6.2 Senior Information Risk Owner (SIRO)

Deans and Directors will appoint Senior Information Risk Owners who will be responsible for being the focal point within their Faculties or Directorates for the escalation and resolution of identified information security risks. SIROs will be responsible for making risk based decisions on requests or changes that are outside of normal working practices or that are exceptions to policy. In the event that the SIRO accepts the request or change they will become the owner of the associated risk.

6.3 Information Security Manager

The Information Security Manager is responsible for:

- creating, reviewing and maintaining information security policies and guidance;
- monitoring and reporting on information security within the University;
- undertaking risk assessments of key information assets;
- evaluating security technologies, processes and the implementation of appropriate levels of security control;
- assessing the adequacy of information security controls for new or changed systems/services;
- providing an advisory service on information security; and
- investigating suspected or actual security incidents.

6.4 Information Security Steering Committee

The Information Security and Information Governance Steering Committee considers all matters concerning the management of information security and information governance. The committee reports to the University Executive Committee. The committee comprises of representatives from each Directorate/Faculty appointed by the Director/Dean and senior institutional information security leads. The committee:

- considers information security, data protection and freedom of information policies and guidance documents prior to submission to the University Executive Committee (and Council where applicable);
- evaluates and reports on the potential impact of proposed information governance and security controls on all areas of the University;
- reviews and monitors information security incidents and data protection breaches and the implementation of any actions which arise;
- identifies and reports on new potential information security risks;
- reviews the implementation and effectiveness of the Information Security Management System components and information governance requirements;
- identifies and oversees training requirements to increase staff awareness of the Data Protection Act, the Freedom of Information Act and other information security matters;
- reviews information security and information governance audit findings and recommendations and monitors the implementation of those recommendations;
- promotes the effective management of all University information, in all formats, to meet both the needs of the University and legislative requirements; and
- promotes a University-wide culture which promotes personal accountability for the appropriate management of information.

6.5 Heads of Department and Line Managers

Heads of Department and line managers are responsible for ensuring that their members of staff:

- have the correct level of access to data assets;
- have read and understood the University's information security and data protection policies and guidance;
- comply with the University's information security and data protection policies and guidance; and
- have undertaken the appropriate information security training.

Line managers are responsible for informing the IT Service Desk promptly if a member of their staff is to cease employment, change role or move to another department.

Line managers will investigate in a timely manner any security concerns that their staff may have and if necessary report them to the Deputy Director of Finance & IT and the Information Security Manager.

6.6 All Staff, Students and Third Party Visitors and Contractors

All the University's system users are responsible for complying with the University's information security policies and guidance. All University system users will sign the IT conditions of use before being supplied with their network account credentials. Users are responsible for reporting any suspected security incidents immediately to the IT Service Desk or if appropriate to their line manager.

Appendix A

List of relevant legislation includes but is not limited to:

- Obscene Publications Act 1959 http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
- Obscene Publications Act 1964 www.legislation.gov.uk/ukpga/1964/74
- Protection of Children Act 1978 www.legislation.gov.uk/ukpga/1978/37/contents
- Police and Criminal Evidence Act 1984 www.legislation.gov.uk/ukpga/1984/60/contents
- Copyright, Designs and Patents Act 1988 www.legislation.gov.uk/ukpga/1988/48/contents
- Criminal Justice and Immigration Act 2008 www.legislation.gov.uk/ukpga/2008/4/contents
- Computer Misuse Act 1990 www.legislation.gov.uk/ukpga/1990/18/contents
- Counter Terrorism and Security Act 2015 (Prevent) http://www.legislation.gov.uk/ukpga/2015/6/contents/enacted
- Human Rights Act 1998 www.legislation.gov.uk/ukpga/1998/42/contents
- Data Protection Act 1998 www.legislation.gov.uk/ukpga/1998/29/contents
- Regulation of Investigatory Powers Act 2000 www.legislation.gov.uk/ukpga/2000/23/contents
- Prevention of Terrorism Act 2005 www.legislation.gov.uk/ukpga/2005/2/contents
- Terrorism Act 2006 www.legislation.gov.uk/ukpga/2006/11/contents
- Police and Justice Act 2006 www.legislation.gov.uk/ukpga/2006/48/contents
- Freedom of Information Act 2000 www.legislation.gov.uk/ukpga/2000/36/contents
- Freedom of Information (Scotland) Act 2002 www.legislation.gov.uk/asp/2002/13/contents
- Equality Act 2010 www.legislation.gov.uk/ukpga/2010/15/contents
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) www.legislation.gov.uk/uksi/2003/2426/contents/made
- Defamation Act 1996 www.legislation.gov.uk/ukpga/1996/31/contents
- Defamation Act 2013 www.legislation.gov.uk/ukpga/2013/26/contents