Information Security Policy v2.1

Organisation	Oxford Brookes University
Title	Information Security Policy
Creator	Information Security Working Group
Approvals Required	1. Information Security Working Group 2. CIO 3. VCG
Version	Version 2.1
Owner	CIO
Subject	The formal approved information security policy of Oxford Brookes University
Rights	Public
Review date and responsibility	Annually by Information Security Working Group

Revision History			
Date	Author	Version Number	Comments
01/05/01	R. Cooke	0.1 (draft)	Original draft
23/04/12	R. Cooke	0.2 (draft)	Updates following ISWG feedback
03/10/12	R. Cooke	0.3 (draft)	Updates following CIO feedback
26/11/12	R. Cooke	0.4 (draft)	Minor amendments only
17/05/13	R. Cooke	0.5 (draft)	Minor amendments only
03/07/13	R. Cooke	1.0 (previous version)	Transition to live
17/03/16	G. Packham	2.0 (previous version)	Updates to terminology
17/03/19	G. Packham	2.1 (live)	Minor amendments only

1. Introduction

Oxford Brookes University recognises that information and its associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, the University will facilitate the secure and uninterrupted flow of information, both within the University and in external communications. The University believes that security is an integral part of the information sharing which is essential to academic and corporate endeavour and this Policy is intended to support information security measures throughout the University.

2. Definition

2.1 For the purposes of this document, information security is defined as the preservation of:

- confidentiality: protecting information from unauthorised access and disclosure;
- integrity: safeguarding the accuracy and completeness of information and processing methods;
- availability: ensuring that information and associated services are available to authorised users when required.

2.2 Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

3. Protection of Personal Data

The University holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes. When handling such information, the University, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 ('the Act'). Responsibilities under the Act are set out in the Data Protection & Privacy Policy - See https://www.brookes.ac.uk/it/information-management/policies-procedures-legislation/

4. Information Security Responsibilities

4.1 The University believes that information security is the responsibility of all students and members of staff. Every person handling information or using University information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the University.

4.2 This Policy is the responsibility of the Chief Information Officer; supervision of the Policy will be undertaken by the Vice Chancellor's Group where appropriate. This policy may be supplemented by more detailed interpretation for specific sites, systems and services. Implementation of information security policy is managed through the Information Security Working Group and Head of Information Security Management.

4.3 The University's IT Services directorate has operational responsibility for the University's IT systems and will therefore take action wherever necessary to protect those systems.

5. Information Security Education and Training

The University recognises the need for all staff, students and other users of University systems to be aware of information security threats and concerns, and to be equipped to support University security policy in the course of their normal work. The Information Security team shall provide appropriate mandatory training on data protection and information security awareness.

6. Compliance with Legal and Contractual Requirements

6.1 Authorised Use: University IT facilities must only be used for authorised purposes. The University may from time to time monitor or investigate usage of IT facilities; and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

6.2 Monitoring of Operational Logs: The University shall only permit the inspection and monitoring of operational logs by appropriate IT Services staff or where it has been otherwise authorised. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur (i) when required by or consistent with law; (ii) when there is reason to believe that a violation of law or of a University policy has taken place; or (iii) when there are compelling circumstances (circumstances where failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policies).

6.3 Access to University Records: In general, the privacy of users' files will be respected but the University reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with University policies and regulations, and to determine which records are essential for the University to function administratively or to meet its teaching obligations. Except in emergency circumstances, authorisation for access must be obtained from the Chief Information Officer (or appropriate deputy) or the University Registrar, and shall be limited to the least access necessary to resolve the situation.

6.4 Protection of Software: To ensure that all software and licensed products used within the University comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts, the University may carry out checks from time to time to ensure that only authorised products

are being used. Unauthorised copying of software or use of unauthorised products by staff or students may be grounds for disciplinary, and where appropriate, legal proceedings.

6.5 Malware prevention: The University will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of electronic devices issued by the University or used for University business shall comply with best practice, as determined from time to time by IT Services, in order to ensure that malware protection is maintained.

6.6 For further information please refer to the University's IT Acceptable Use Policy.

7. Asset Management

All University information assets (data, software, computer and communications equipment) shall be accounted for and have a designated owner. The owner shall be responsible for the maintenance and the protection of the asset/s concerned.

8. Physical and Environmental Security

Physical security and environmental controls must be appropriate for identified risks. In particular, critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls.

9. Information Systems Acquisition, Development and Maintenance

9.1 Information security risks must be identified at the earliest stage in the development of business requirements for new information systems or enhancements to existing information systems.

9.2 Controls to mitigate the risks must be identified and implemented where appropriate.

9.3 For further information please refer to the University's Third Party Supplier Security Management policy.

10. Access Control

10.1 Access to information and information systems must be driven by business requirements and be commensurate and proportionate to the business need.

10.2 A formal access control procedure shall be required for access to all information

systems and services.

10.3 For further information please refer to the University's IT Access Control policy.

11. Communications and Operations Management

Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities must be established.

12. Retention and Disposal of Information

All staff have a responsibility to consider security when disposing of information in the course of their work. Owners of information assets should establish procedures appropriate to the information held and processed and ensure that all staff are aware of those procedures. Retention periods should be set in consultation with the University Records Manager.

13. Incident Reporting

All staff, students and other users should report immediately via the Servicedesk portal (https://service.brookes.ac.uk/Brookes), or by telephone to the Service Desk on tel. ext. 3311, any observed or suspected security incidents where a breach of the University's security policies has or may have occurred, and any security weaknesses in, or threats to, systems or services.

14. Business Continuity

14.1 The University will implement, and regularly update, a business continuity management process to counteract interruptions to normal University activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

14.2 Business continuity planning shall consider information security requirements and regularly test plans to ensure that they are effective.