Information Security Policy

Version	3.0
Reviewed Date	15/06/2023

Contents

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.

This policy should be read in conjunction with all other relevant policies, regulations and guidance published by the University.

This policy supports compliance with the information security standards IEC/ISO 27001:2013 and PCI DSS.

2. Definition

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

(i) confidentiality: protecting information from unauthorised access and disclosure.

(ii) integrity: safeguarding the accuracy and completeness of information and processing methods.

(iii) 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, photographs, video image, audio recording 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 law. Responsibilities under the Data Protection Act and other relevant legal provisions are set out in the Data Protection & Privacy Policy (here)

4. Information Security Responsibilities

4.1 The University is committed to introducing, maintaining and continually improving the information security management system (ISMS) and all things related to this. It 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 Head of Information Security Management; 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 (ISWG) and the 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

5.1 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 - Legal & 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 by the Head of Information Security Management or nominated deputy. Disclosure of information from such logs, to the Police 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, or other compelling reason).

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 as well as 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

7.1. 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

8.1 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 suitable for risk identified.

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 and risk treatments plans devised.

9.2 The responsibility for identifying and documenting any risks sits with the project or programme lead.

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

9.4 For further information see the 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 is required to cover the 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.

Staff must be aware of any legal requirements regarding how long data must be kept for and then by default apply the University's records management policy, when determining how long to retain data.

13. Incident Reporting

All staff, students and other users should report immediately via the Service Desk 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. This includes but is not restricted to a data breach.

Staff must be familiar with the Information Security Incident Management Policy which sets out the process to follow where there is an actual incident or a near miss.

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.

15. Setting of security objectives for the ISMS

15.1 Top management shall establish or adopt a framework for the setting of security objectives and these will be shared with relevant parties.

15.2 . Security objectives are identified from different areas: such as guidance from regulators, changes in standards from certified bodies, risk raised by interested parties, changes in the organisation and changes external to the organisations, for example environmental, commercial, legal and community and third party agents the university employs as goods or service providers, and technological.

16. Continual improvement within the ISMS

16.1 Top leadership will ensure robust programmes of continual improvement are delivered by supporting from the top down implementation of such programmes necessary to continually improve upon the operational status of the information security management system (ISMS).