

Information Access and Security Policy

1 Introduction

- 1.1 Information is fundamental to the University's core activities. The Information Access and Security Policy defines the University's overall policy in relation to the creation, evaluation, dissemination and exploitation of information within the University. It aims to assist the University to operate effectively and efficiently, to comply with legislation and good practice, and to safeguard its information assets against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence. The Information Access and Security Policy is supported by more detailed policies and guidelines in specific areas.
- 1.2 The Information Access and Security Policy covers all information owned or processed by, or on behalf of, the University, regardless of its location and the physical medium on which it is stored, e.g. paper, electronic, or microform.

2 Principles

- 2.1 The Policy operates on the basis of the following principles:
 - relevant, accurate, up-to-date and timely information should be readily and widely accessible where practicable, within a framework of appropriate security
 - all information created or acquired through University funds is owned by the University
 - a designated custodian should be responsible for its operational integrity and for implementing the access policy
 - intellectual property is governed by the University's regulations on intellectual property.
- 2.2 These principles of *access, ownership, and intellectual property* are articulated in the University's *Information Strategy 2004-2009*.
- 2.3 Rights of access to information are balanced by responsibilities: the University will have policies and regulations in place, and will define procedures and provide mechanisms to ensure that information is handled within the appropriate laws and codes of practice; individuals must operate within this environment and are accountable for their actions.

3 People

- 3.1 The Policy applies to all those - staff, students, associates and agents - who handle University information as part of the University's business. Visitors to the University, who have access in person or electronically, should be made aware of the Policy insofar as it affects them. Collaborators, for instance in research partnerships, or agents with whom the University or individuals have a contractual relationship, must similarly be made aware of University policies, guidelines or codes of practice relating to information. Anyone entering into a contract on behalf of the University must ensure compliance with this Policy.

4 Access

4.1 Rights of access

4.1.1 The University will provide easy access to information to enable those operating on its behalf to undertake their duties effectively; this information will include information generated and owned by the University as well as appropriate external information. In addition, the University will provide access to internal information to external bodies and individuals under the terms of the Freedom of Information Act and to those with whom the University has statutory or contractual commitments. The University will protect the rights of individuals in relation to access to personal and/or sensitive data held by the University, both under Data Protection and Human Rights legislation and in compliance with the University's ethical framework. Physical and/or electronic access control systems will be provided to ensure that access to personal and/or sensitive information is available only to authorised individuals. The University will ensure that clear guidelines are provided on the deployment of personal and/or sensitive information and will provide training in their deployment.

4.2 Constraints on access

4.2.1 In addition to the legal constraints on access to specific items of information, the University has developed policies and guidelines to ensure confidentiality, to reflect good practice, and to maintain sensitive information. These are detailed under Responsibilities below and in Appendix 1.

5 Responsibilities

5.1 The misuse and abuse of information may have serious implications for the University both in legal sanctions and in damage to the University's reputation. In some cases the individual processing the information has a personal legal liability in addition to the liability of the University. The University will produce guidelines for processing of information where specific liabilities may arise, but the University expects all those handling information on its behalf to do so in a responsible manner. The main legislation and university guidance areas are detailed below and in Appendix 1.

5.2 The University and individuals as information providers and users have responsibilities to manage the access to and the security of information, within laws, policies, guidelines and codes of practice. The Records Manager has overall responsibility for record-keeping and use. There will be a custodian (normally the person who created or commissioned the information or a nominee) for each item of information created or held by the University and its members who is responsible for ensuring its integrity and accuracy, for legal compliance, for determining access rights, and for carrying out risk assessments on the value and security of the information. Each individual is responsible for his or her actions and should not take any action which they know to be outside the law or in breach of University policies, guidelines or codes of conduct. Heads of Department are responsible for the implementation and monitoring of the Policy within their departments and for ensuring that those for whom they are responsible, including visitors and contractors, are aware of the Policy and associated guidelines.

5.3 Information should be provided, held, managed, and disposed of, within the relevant laws and regulations in force, including the following: Data Protection, Freedom of Information, Human

Rights, Disability Discrimination, Copyright Designs and Patents, Computer Misuse, Telecommunications, Pornography, Children's Act, Regulation of Investigatory Powers, Sex Discrimination, Racial Discrimination, Environmental Information, and Health and Safety at Work. The University will provide information or guidelines, as appropriate, on relevant legislation or regulations, though individuals have a responsibility to ensure that they are operating within the law.

- 5.4 Policies, guidelines, and codes of practice must be adhered to. These may be issued by the University or by professional bodies with which the University has an association, the Joint Information Systems Committee (JISC), or the United Kingdom Education and Research Networking Association (UKERNA) etc. Relevant documents or codes are listed in the appendix.
- 5.5 Mechanisms will be provided by the University where appropriate or by the custodian of the information to help ensure that information may be used only within the laws or regulations pertaining to it. Such mechanisms may be physical, such as locking cabinets, or virtual, such as password control. Similarly, the University will carry out its responsibilities in relation to security by authorisation, physical and electronic access control, and processing procedures.

6 Copyright, Licensing and Intellectual Property

- 6.1.1 All information in the UK is governed by the laws of copyright, specifically the Copyright Designs and Patents Act 1988, and any subsequent regulations emanating from the European Union which bind all member states. Copyright laws vary in other countries, notably in the United States, and individuals must take appropriate steps to ensure compliance.
- 6.1.2 Further conditions apply through licensing of information storage and copying, where the University may pay a licence or indemnity to a third party. Relevant licences include those administered by the Design and Artists Copyright Society (for slide production and holdings), Newspaper Licensing Agency (for copying of parts of newspapers), the Copyright Licensing Agency (for copying of articles and parts of books beyond those currently accepted for personal use under the 'fair dealing' clauses of the Copyright Designs and Patents Act 1988).
- 6.1.3 Computer software and operating systems, and access to electronic information resources, are normally provided under licence. Where University-wide licences are provided, usually through the Computing Service or the Library, members of the University must comply with the terms of the licence; in purchasing software etc for themselves or their research groups on behalf of the University they must also ensure compliance. The University will produce guidelines for software and database licensing, having regard to the general licensing conditions for the Higher Education community defined in the CHEST code of conduct. Care must be taken in downloading or printing information from the Internet, or in sharing software packages, that such actions are within the terms of the law or licences. In cases of doubt, permission of the copyright or licence holder should be sought.
- 6.1.4 Intellectual property rights are determined and protected by University Regulation 12.

7 Security

7.1 Rights to security

7.1.1 The University is committed to providing a secure environment in which information can be accessed and processed. Subject to disclosure under court order, data subjects have legal rights to confidentiality of information held about them by the University, and personal or sensitive information will be available only to those authorised.

7.2 Data security

7.2.1 The custodian of the information has a duty to ensure data security through appropriate procedures and mechanisms, including electronic authentication, which provide controlled access to the information only to appropriately authorised people. S/he must ensure, insofar as is possible, the accuracy and currency of information, and must take reasonable steps to maintain data integrity for information held in physical or in electronic form. In order to prevent corruption or loss of data, the custodian must ensure that reliable backup procedures are instituted. Restoration procedures following backup must be tried and tested. The University will provide guidance via the Computing Service.

7.2.2 Arrangements will be made for archiving material as needed (within the Data Protection Act), with attention given to retention schedules and secure storage.

7.2.3 The University will institute a policy and procedures for secure disposal which must be used for the disposal of sensitive material, include information relating to personnel, University committee papers or financial documents. Computing equipment holding University data or licensed software must be disposed of responsibly, ensuring that hard disks are wiped or reformatted, so that no data can subsequently be retrieved.

7.3 Computer and network security

7.3.1 The University will take reasonable steps to ensure the integrity of its computer systems and data communications network. In particular, the University will implement access controls to the University's network from the Internet via a firewall and will control external access from the campus network. The University will develop a policy together with associated mechanisms for accessing University information from home or from other off-campus locations. Facilities for virus detection and control will be provided. Access to individual servers will normally require authorisation and authentication via passwords, but the University will, as far as is practicable, implement a single sign-on for access to central servers. Heads of Department will be responsible for the security of departmental systems, including ensuring that operating environments take advantage of the latest security patches, and the University will provide guidance on best practice. The University will continue to take advantage of appropriate technologies to improve access control and ease of use, e.g. digital signatures, encryption, and bio-authentication.

8 General

8.1 Standards

8.1.1 The University will adhere to appropriate national and international standards in deploying technology, consistent with the requirements of a research environment; the major standards will be identified in the University's Information Technology Strategy. In addition, the University will comply with appropriate codes of conduct and good practice developed by the higher education community, appropriate professional bodies, or by those bodies with which it collaborates e.g. the NHS. The University will have regard to the British Standard: *Code of Practice for Information Security Management*, BS7799 in defining information management procedures and guidelines.

8.2 Audit

8.2.1 Head of Departments are responsible for ensuring that appropriate strategies and procedures relating to information are in place at departmental level, and to ensure effective operation after a disruptive incident in accordance with the University's Business Continuity strategy. Policies and procedures relating to information held or managed within the University will be audited and reviewed regularly by Information Committee or other appropriate body.

8.3 Finance and funding

8.3.1 Responsibility for implementing and abiding by this policy resides with Information Committee, Departments and individuals. The University will devote central or departmental funding as appropriate for the implementation and operation of the Policy, and will monitor implementation by reporting through central and departmental plans.

8.4 Complaints Procedures

8.4.1 Alleged contraventions of the legislation and the University's policies, guidelines or codes of practice, or alleged breaches of security should be submitted via the appropriate University complaints or grievance procedure. Alternatively, specific points of contact may be identified to obtain more detailed guidance or to carry out a preliminary investigation.

Appendix 1 - Related policies and guidelines

Topic	Policies and guidelines	Location of document (url)	Responsibility (to carry out)
2 Principles	Information Strategy University Regulation 12: Intellectual Property	http://www.york.ac.uk/admin/po/infostrat.yrk/ http://www.york.ac.uk/admin/aso/ordreg/r12.htm	Information Committee HoDs, individuals
2.3 Responsibilities	Legislation		HoDs, individuals
4 Access. 4.1 Rights of access	Legislation Data Protection policy	www.york.ac.uk/admin/dpc/dppolicy2002.htm	HoDs, individuals
5 Responsibilities	Legislation University policies - various e.g. equal opportunities Internal Communication Strategy	http://www.york.ac.uk/admin/aso/eqopps/strategy.htm http://www.york.ac.uk/admin/presspr/intcomstrategy.htm	University, HoDs, individuals
6 Copyright	<i>Copyright, Designs and Patents Act 1988</i> Newspaper Licensing Agency Copyright Licensing Agency University Regulation 12 CHEST Code of Conduct	http://www.york.ac.uk/admin/aso/ordreg/r12.htm http://www.york.ac.uk/coord/docs/regs/defed.htm	HoDs, individuals
7 Security. 7.1 Rights	Legislation		University, HoDs, individuals
7.2 Data security	Data Protection policy	www.york.ac.uk/admin/dpc/dppolicy	HoDs, individuals

		cy2002.htm	
7.3 Computer and network security	JANET Acceptable Use Policy Student Network Service - Terms and Conditions	http://www.york.ac.uk/services/cserv/offdocs/juse.htm http://www.sns.york.ac.uk/tandc.html	HoDs, individuals Individuals
8 General. 8.1 Standards	British Standard. <i>Code of practice for information security management</i> , BS7799		
8.2 Audit			Information Committee, HoDs
8.3 Finance and funding			Information Committee, HoDs
8.4 Complaints procedure	various		Registrar

Appendix 2

Information Access and Security Policy

The Information Access and Security Policy has been revised in the light of recent strategy and policy documents.

The following policies and guidelines are under development

Policy or guidelines	Responsibility for production
Business Continuity Strategy	DFM
Freedom of Information	Registrar
Computer and network security guidelines	Computing Service
YIMS Systems Security and Access Control Policy	SIP Steering Group
Guidelines on software and licensing	Computing Service
Remote access to University information resources	Computing Service
Secure disposal of data and computing equipment	Computing Service