

20/12/07

University of Bristol Information Access & Security Policy

1 Introduction

Information is a vital asset to any organisation, and this is especially so in a knowledge-driven organisation such as the University, where information will relate to learning and teaching, research, administration and management. This policy is concerned with information held in the University and used by members of the University in their official capacities, for example as staff or students. It relates to both computer-based and paper-based information. The policy defines the responsibilities of individuals with respect to information use and to the provision and use of information processing systems.

2 Information Access & Security principles

The University has adopted the following principles, which underpin this policy:

- ❑ Information will be protected in line with relevant laws and University policies, notably those relating to data protection and freedom of information.
- ❑ Information should be available to all who have a legitimate need for it.
- ❑ Information must be classified according to an appropriate level of availability: public, open (within the University), confidential, strictly confidential or secret.
- ❑ Integrity of information must be maintained; information must be accurate, complete, timely and consistent with other information.
- ❑ All who have access to information have a responsibility to handle it appropriately according to its classification.
- ❑ Nominated staff of the University are responsible for ensuring that appropriate procedures and systems for the processing and holding of information are in place and are effective.
- ❑ Information will be protected against unauthorised access, inappropriate for its classification.
- ❑ Data backup and recovery and business continuity plans will be produced, tested and maintained, to ensure that vital information services are available within defined service levels.
- ❑ Compliance with this policy will be enforced. Breaches of information security controls must be reported to and will be investigated by the Information Security Officer.

Appropriate information access and security involves knowing what information exists, permitting access to all who have a legitimate need and ensuring the proper and appropriate handling of information.

3 Definitions

Information	Information takes many forms and includes data stored on computers, transmitted across computer networks, printed, written, sent by post or fax, or stored on tapes or discs. Information may be either structured according to some defined format, or unstructured.
Access	Access refers to mechanisms, whether legitimate or not, by which individuals gain access to information. The policy defines legitimate access and prescribes action to be taken to deal with unauthorised access.
Security	Security refers to mechanisms and procedures designed to ensure that appropriate controls on information access are in place and are effective.
Confidentiality	Confidentiality requires protection of information from unauthorised disclosure or intelligible interception (see below).
Integrity	Integrity involves safeguarding the accuracy, completeness and consistency of information and of computer software.
Availability	Availability involves ensuring that information and vital services are available to users when required.
Intelligible interception	Intelligible interception is interception of information in such a way that it is readable; encryption of data may prevent intelligible interception.
Information assets	Information (as defined above), computer software and hardware, computer systems

This Information Access and Security policy may be summarised as the preservation of confidentiality, integrity and availability, in line with the principles set out in BS7799.

4 Legal obligations and University policies

The policy should be read in conjunction with contracts of employment, university policies relating to the usage of information and systems, and relevant legislation, including:

- Policies on data protection and freedom of information
- Policies on disclosure of criminal records
- Regulations for the use of computer facilities (incorporating the JANET Acceptable Use policy)
- Policy for the investigation of computers and disposal of computer equipment

- Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Freedom of Information Act 2000, Computer Misuse Act 1990, Copyright, Design and Patents Act 1988, Official Secrets Acts 1911-1989
- The Terrorism Act 2000, The Anti-Terrorism, Crime and Security Act 2001.

5 Information classification

On advice from the University's Information Access Adviser (who advises on matters including data protection, freedom of information and records management), all information in the University will be classified by those responsible for the information into one of the following categories. Any disagreement as to classification will be resolved by the University Secretary.

Public	May be viewed by anyone, anywhere in the world.
Open	Available to all members of the University, but not to others.
Confidential	Available only to specified members of the University, with appropriate authorisation.
Strictly Confidential	Access is controlled and restricted to a small number of people.
Secret	For example, subject to or obtained under the Official Secrets Act.

Much information will fall into the public or open categories, but for good reason, such as personal privacy or protection of University interests, some information will be categorised as confidential or strictly confidential.

Information may also be categorised as either current, up to date and accurate, or historic, but held for good reason as a record. Historic information may be archived (i.e. retained but removed from prime information sources and possibly stored in a pared down form). Information must be deleted when there is no valid reason for retention. Disposal must be considered when the information is first acquired, as set out in the data protection policy.

6 Access to information

All information will be classified as described above. Individuals will have access to information according to its classification. Appendix 1 sets out a high level information access matrix; this is not exhaustive. Data guardians will be responsible to the Information Access Adviser for ensuring that all information is appropriately classified and for ensuring the review and maintenance of information classification. The Information Access Advisor will oversee this process and will maintain the high level matrix (appendix 1). The University Secretary will be the final arbiter on issues relating to information classification and access. See below for definitions of Data Guardian, Information Access Adviser and other roles.

7 Roles & Responsibilities

All members of the University have responsibilities with respect to information, as summarised below. One person often has more than one role. In order to fulfil these responsibilities, members of the University must:

- ❑ be aware of this policy and comply with it
- ❑ understand to which information they have a right of access
- ❑ know the information for which they are guardians
- ❑ know the information systems and computer hardware for which they are responsible

Members of the University as information users

All members of the University will be users of information. This carries with it a responsibility to abide by this policy and related policies and laws. No individual should be able to access information to which they do not have a legitimate access right. Systems should be in place to provide controls, but not withstanding this, no individual should knowingly contravene this policy, nor allow others to do so.

Information users must be aware of the nature of the information to which they have access must handle information appropriately, especially according to its classification. Information must protect the confidentiality of information and must not deliberately or inadvertently give access to others who do not have legitimate access. Examples of inadvertent access could include leaving confidential printed material where others might see it or leaving data visible on a computer screen where others might see it.

Data guardians

Many members of the University will have responsibility for the confidentiality, integrity and availability of information, for example:

- ❑ Heads of department are responsible for the confidentiality, integrity and availability of information maintained by members of the department, such as students' academic records. They are responsible overall for technical aspects of departmental information systems.
- ❑ Departmental administrators, departmental IT support staff and other staff in departments will have delegated authority from heads of department.
- ❑ Data and systems managers in support services are responsible for the confidentiality, integrity and availability of corporate information, such as student, personnel and financial data.
- ❑ Project managers (or equivalent), leading projects for the development or modification of information systems, are responsible for ensuring that projects take account of the needs of information access and security and that appropriate control mechanisms are instituted and are effective, so that the confidentiality, integrity and availability of information is guaranteed.

Systems administrators

Computer systems administrators are responsible for ensuring that computer systems are effectively managed, to ensure information confidentiality, integrity and availability. This includes ensuring proper user administration (access controls, security mechanisms) and data administration (access controls, security mechanisms, backup, safe disposal etc).

Information Services staff

Information Services staff are responsible for ensuring that provision of University IT infrastructure is consistent with the demands arising out of this policy.

The Assistant Director of Information Services (Information Systems & Computing) is responsible overall for ensuring the technical delivery of policy objectives with respect to the University and for provision of advice, guidance and where appropriate, direction to Heads of Department and departmental IT Support Staff.

The Information Security Officer is responsible for compliance, investigating actual, potential or suspected breaches of this policy, typically from a technical perspective.

University Secretary's Office

The Information Rights Manager is responsible for the appropriate classification of information and that the classification scheme is publicly available.

The University Secretary is responsible for enforcement of this policy and for disciplinary procedures resulting from non-compliance.

8 Compliance

Compliance with this policy will be enforced according to University disciplinary procedures, which are overseen by the University Secretary. The Information Security Officer will advise the University Secretary and other senior managers on matters relating to compliance. Attention is drawn to laws and policies previously listed. Users should only access and use information for which they have appropriate authorisation and which is classified as being available to them. Usage of information must be in an appropriate manner. Usage of systems and software must be in accordance with policies, laws and licensing constraints, and specific attention should be paid to copyright laws and licence agreements. In certain circumstances, the University will investigate the usage of information and information processing systems, and specific attention is drawn to the policy for the investigation of computers.

9 Incident handling

Any member of the University must report any information security incident to one of the following, or use the University's public interest disclosure policy:

Information Security Officer, Computer Centre, Tyndall Avenue, Bristol

Telephone: 0117 928 7849

Email: cert@bristol.ac.uk

The University Secretary, Senate House, Tyndall Avenue, Bristol
Telephone: 0117 928 7788
e-mail: university-secretary@bristol.ac.uk

Incidents will be investigated (in accordance with the published incident response procedure) by the Information Security Officer who will report to the University Secretary and/or to the Assistant Director of Information Services (Information Systems & Computing). The University Secretary will determine whether and what disciplinary action is to be taken. The Assistant Director of Information Services (Information Systems and Computing) will, on advice from the Information Security Officer, ensure that appropriate technical steps are taken to address any technical security weaknesses.

10 Summary of Technical Procedures

Procedures (set out in more detail in Appendix 2) will be put in place in order to ensure effective information access and security control, as follows:

- ❑ User registration procedures, authentication mechanisms and password usage for access to email and other computing facilities
- ❑ Control of and mechanisms for access to University computer networks, network system security, intrusion detection, prevention and remedial action
- ❑ Systems security procedures, including systems administration, monitoring and logging, security patches, virus protection, encryption
- ❑ Backup of computer systems
- ❑ Inventory of information assets, including equipment, software and data
- ❑ Systems change control, testing and acceptance
- ❑ Information access control for different classifications of information, database administration, regular review of user access rights
- ❑ Management of special (“super user”) systems privileges and utilities
- ❑ Disaster recovery and business continuity
- ❑ Physical security of computer rooms, networks, personal computers, computer maintenance and disposal
- ❑ Audit

The objective of these technical procedures is to ensure that:

- ❑ Information users are appropriately identified and have access to information for which they have a legitimate need
- ❑ Computer systems are appropriately managed and controlled in line with the requirements of this policy
- ❑ Information assets are identified and protected
- ❑ There is clear assignment of responsibilities

Appendices

- 1 Information Matrix:** <http://www.bris.ac.uk/WorkingGroups/CITG/infomatrix.pdf>
- 2 Technical Procedures:** <http://www.bristol.ac.uk/WorkingGroups/CITG/IASPolicyappendix2public.pdf>
- 3 References:** <http://www.bristol.ac.uk/WorkingGroups/CITG/IASPolicyappendix3.pdf>