University of Liverpool

Information Security Policy

Reference Number	CSD-003
Title	Information Security Policy
Version Number	3.0
Document Status	Active
Document Classification	Open
Effective Date	01 October 2011
Review Date	01 September 2017
Author	John Cartwright, Chris Wooff, Steve Aldridge, Sue Byrne
Approved by	Council 28 November 2011
Implemented by	Information Security Officer
Monitoring of compliance	Faculty Information Security Managers
Comments	• 01/09/2015 - Annual Review – No changes to current Version • 07/09/2016 – Appendix A under review

Information Security Policy

Table of Contents

1. Introduction

Information is a vital asset to any organisation, and this is especially so in a University which is a knowledge-driven organisation, where information relates to learning and teaching, research, intellectual property arising from research, consultancy, administration and management. This policy is concerned with information held by 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. This policy defines the responsibilities of individuals with respect to information use and to the provision and use of information processing systems.

This Information Security policy can be summarised as the preservation of confidentiality, integrity and availability which is informed by the principles set out in IS0 27001.

All members of the University are directly responsible and liable for the information they handle. Failure to comply with this policy, and other associated policies, may result in disciplinary action.

Management Commitment;

> *"All of our key priorities require enhanced information enablers, giving users access to up-to-date information to support their specific activities. With this access comes a responsibility for users to ensure the information is used and maintained in a secure and appropriate way. This policy and associated policies, codes of practice and guidance notes are provided to help you meet your responsibility and protect our Institution. The senior management of the University fully support the principles and practices defined within this Information Security Policy".*
>
> *…. Patrick Hackett – Chief Operating Officer*

2. Principles

Appropriate information security involves knowing what information exists, permitting access to all who have a legitimate need and ensuring the proper and appropriate handling of information. The University has adopted the following principles, which underpin this policy:

- Information will be protected in line with relevant laws and University policies, particularly 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 members of the University who have access to information have a responsibility to handle it appropriately, according to its classification.
- Nominated University staff 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.
- Service Level Agreements will be produced, tested and maintained, to ensure that vital information services are available within defined service levels.

- Compliance with this policy is compulsory for all staff and students making use of University information. Breaches of information security controls must be reported to, and will be investigated by, the Information Security Officer.

3. Definitions

Information

Information takes many forms. For the purposes of this policy, it includes data stored on computers, transmitted across computer networks, printed, written, sent by post or fax, or stored on removable devices. Much of this policy relates specifically to electronic information but the same principles and level of care should be applied to paper-based information. Information may be either structured according to some defined format, or unstructured.

Access

Access refers to any mechanisms by which individuals gain access to information. This 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 both information and computer software.

Availability

Availability involves ensuring information and the associated services needed to process that information are available to staff and students when required.

Computer Software

Computer software is the collection of computer programs used to process information.

Intelligible interception

Intelligible interception is interception of information in such a way that it is readable. Encryption of data may be used to prevent intelligible interception.

Information assets

Information assets include information (see above definition), computer software and hardware.

User Name

A unique identifier which is allocated to a member of the University and which, together with a password, is used to identify and authenticate access to a system.

4. Legal obligations and University policies

This policy should be read in conjunction with contracts of employment, University policies relating to the usage of information and systems, and relevant legislation. Relevant University policies include:

- Policy on data protection
- Policy on freedom of information.
- Regulations for the Use of IT Facilities at the University of Liverpool (incorporating the JANET Acceptable Use policy).
- Policy for the investigation of computers.
- Policy on the use of laptops and mobile devices.
- Records retention policy

References to each of these policies are to be found in section 12.

Relevant legislation includes:

- Data Protection Act 1998.
- Human Rights Act 1998.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Computer Misuse Act 1990.
- Copyright, Design and Patents Act 1988.
- Copyright (Computer Programs) Regulations 1992.
- The Terrorism Act 2000
- The Anti-Terrorism, Crime and Security Act 2001.
- Official Secrets Acts 1911-1989.
- Obscene Publications Act 1994.

5. Roles and Responsibilities

All members of the University have direct responsibilities for 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 which information they have a right of access to,
- know the information for which they are owners,
- know the information systems and computer hardware for which they are responsible.

Governance

Appendix A provides the governance framework which is used in assigning responsibility for the management of information security.

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 legislation. No individual should be able to access information to which they do not have a legitimate access right. Systems must 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 and must handle information appropriately in accordance with its classification. Information users 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 view it.

Information Owners

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 their department, such as students' academic records. They are also responsible for the security of all departmentally operated information systems. These responsibilities are defined in Appendix B.
- Departmental administrators, departmental IT support staff and other staff in departments may 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 and effective control mechanisms are instituted, 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).

Computing Services staff

The Director of Computing Services has overall responsible 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.

Staff in the Computing Services Department are responsible for ensuring that provision and operation of University IT infrastructure is consistent with the demands of this policy.

Information Security Officer

The Information Security Officer is responsible for compliance, investigating actual, potential or suspected breaches of this policy, typically from a technical perspective. In addition, the Information Security Officer provides support and advice to University departments.

Faculty Information Security Manager

The Faculty Information Security Managers are responsible for the implementation of this policy within their respective faculties. For the purposes of this policy, Professional Services is treated as a faculty.

Data Controller

The Data Controller bears legal responsibility for ensuring that the University meets its legal responsibilities for information security. In accordance with the Data Protecttion Act, the University is the designated data controller. Day to day responsibility for data protection is delegated to the University's Data Protection Officer.

University Records Manager

Many information assets need to be retained for a defined length of time, whether on electronic systems or through other media. This can be dictated by law, regulations, good practice or for organisationally defined business reasons. The University's Records Manager can provide advice on developing appropriate retention policies.

The University's Records Manager is also responsible for managing the Records Centre. This centre offers medium-term storage (5-10 years on average) for a huge range of university records. These are records which are no longer required day-to-day within their originating department but which may be needed occasionally, or have to be retained for financial or legal reasons. The Records Centre informs each department when their records are due for review or destruction and makes a recommendation as to their disposal.

Records Management also runs the University's confidential waste destruction service. This is predominantly for the disposal of paper-based confidential information but non-paper media such as CDs, disks and magnetic tape can also be destroyed through this service.

6. Access to information

All information will be classified as described below. Individuals will have access to information according to its classification. Information owners will be responsible for ensuring that all information is appropriately classified, against defined standards, and for ensuring the review and maintenance of information classification. The University's Chief Operating Officer will be the final arbiter on issues relating to information classification and access.

7. Information classification

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 a faculty information security officer (or their Professional Services equivalent).

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. Note that this IT-based definition of archiving is very different to the one used by Records Management and the University Archives. Information is only classed as archival in this context if it has been designated for permanent preservation in the University archives. Material stored in the University Records Centre is classed as semi-current as it is no longer active in the originating department and a decision has not yet been taken on whether it will be destroyed or archived.). Information must be destroyed 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 (see section 12).

Public
May be viewed by anyone, anywhere in the world.

Open
Access is available to all members of the University who have a legitimate right to access University IT systems via a user name (see section 3).

Confidential
Access is only available to specified members of the University, with appropriate authorisation.

Strictly Confidential
Access is controlled and restricted to a small number of named individuals.

Secret
Access is subject to, or obtained under, the Official Secrets Act.

Retention Schedule
This policy covers all records, regardless of form or medium, which are created, received and/or maintained by the university, its officers and employees in the course of the University's business. Records created, received and/or maintained in these circumstances become University property and subject to the University policy for the retention and disposal of records. The University must retain certain records for operational and administrative purposes and to demonstrate compliance with statutory or regulatory requirements. There are also various legal and operational reasons why information should not be kept for longer than necessary. The Records Management Service will maintain a schedule for each department listing the periods for which each type of record must be retained. These schedules are drawn up in agreement with the heads of the department (or their representative) taking into account any relevant compliance and operational requirements.

8. Compliance
Compliance with this policy will be enforced according to University disciplinary procedures, which are overseen by the Chief Operating Officer.

The Director of Computing Services will advise the Chief Operating Officer and other members of the Professional Services Leadership Team on matters relating to compliance. Faculty Managers will be responsible for cascading this advice to their academic colleagues. Attention is drawn to laws and policies previously listed in section 4. 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 associated 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 (see section 12).

9. Incident Handling
Any member of the University must report any information security incident to their Faculty Information Security Manager (or their Professional Services equivalent).

Incidents will be investigated by the Faculty Information Security Manager who will report to the Information Security Officer and/or to the Director of Computing Services. Where appropriate, the

Chief Operating Officer will determine whether and what disciplinary action is to be taken. The Director of Computing Services will, on advice from the Information Security Officer, ensure that appropriate technical steps are taken to address any technical security weaknesses.

10. Implementation

Procedures will be put in place in order to ensure effective information access and security control. 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

The procedures will include:

- 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 privileged systems access
- Disaster recovery and business continuity, escalated in-line with the Business Continuity Plan
- Physical security of computer rooms, networks, personal computers, computer maintenance and disposal
- Audit procedures to ensure that the use of all IT systems is recorded.

11. Storage of University Computer-based Information

Introduction

It is strongly recommended that all University Computer-based Information Assets are stored on server systems operated by the University's Computing Services Department. The data storage of these systems is resilient to failures; it is backed up on a daily basis to systems also held in secure locations. It is recognised that for some very large data sets (for example terabytes of data collected from experiments) it may be impractical to store this on Computing Services operated systems. However, Computing Services must still be consulted about the storage and management of such data.

Where University Computer-based Information Assets are not stored on servers operated by Computing Services, then the appropriate Head of Department must ensure that appropriate data backup procedures are in place and operational.

Business Systems

For data held within the University's business systems (the Finance System, the Student System, the Estates System and the Payroll & Personnel System), within the virtual learning environment (VITAL) and on the corporate Web, the user need take no specific action; these systems automatically store the information in databases that are held on Computing Services managed servers.

Email System

Data held within the University's email system is secure and backed up on a daily basis. University Computer-based Information Assets should not be stored only within the email system: the primary copy of any such Information Asset should be stored on the Managed Windows Service.

Managed Window Service

Computer-based Information Assets that originate on PC or similar systems (including Word Documents, Spreadsheets and Access databases) should be stored on a network drive hosted on a Computing Services Managed Windows Service (MWS).

All registered computer users are provided with a network drive as part of their registration for Computing Services. Most users make use of the MWS and this network drive is accessible as the M: drive whenever the user is logged on to the MWS. For individuals that do not use the MWS, or use the MWS in Standalone mode, other ways are provided for using this disk space. Users should therefore store University Information Assets on the M: drive and not on the local hard disk drive of their machine. Access to the M: drive space is secure: it requires the user name and password of the owner to access the file space. By default, no other user has access to the data. Other users may be granted access to individual folders (or even files) within the M: drive; they will only have access to the data to which the owner has granted access and need to give their own username and password when accessing the shared information.

Use of Desktop PC Storage

Computer-based Information Assets held on PCs or other systems in offices or laboratories are not normally secure against theft, damage due to fire, flood or vandalism, or other incidents. The information held on these systems must be secured to ensure that anyone who gains unauthorised access to the physical machine cannot obtain access to the information stored on its hard disk. Information held on these systems must also be backed up on a regular basis and the backups should be tested (to ensure that the data can be restored).

University Information Assets must not be stored on desktop PCs which are located on non-University premises. In particular, this includes home systems.

Use of Laptop Storage

University Computer-based Information Assets held on laptop and portable systems must be encrypted and should also be stored on the user's M: drive. The user must establish a working regime that copies changed data onto their M: drive on a regular basis so as not to put the University's information "at risk".

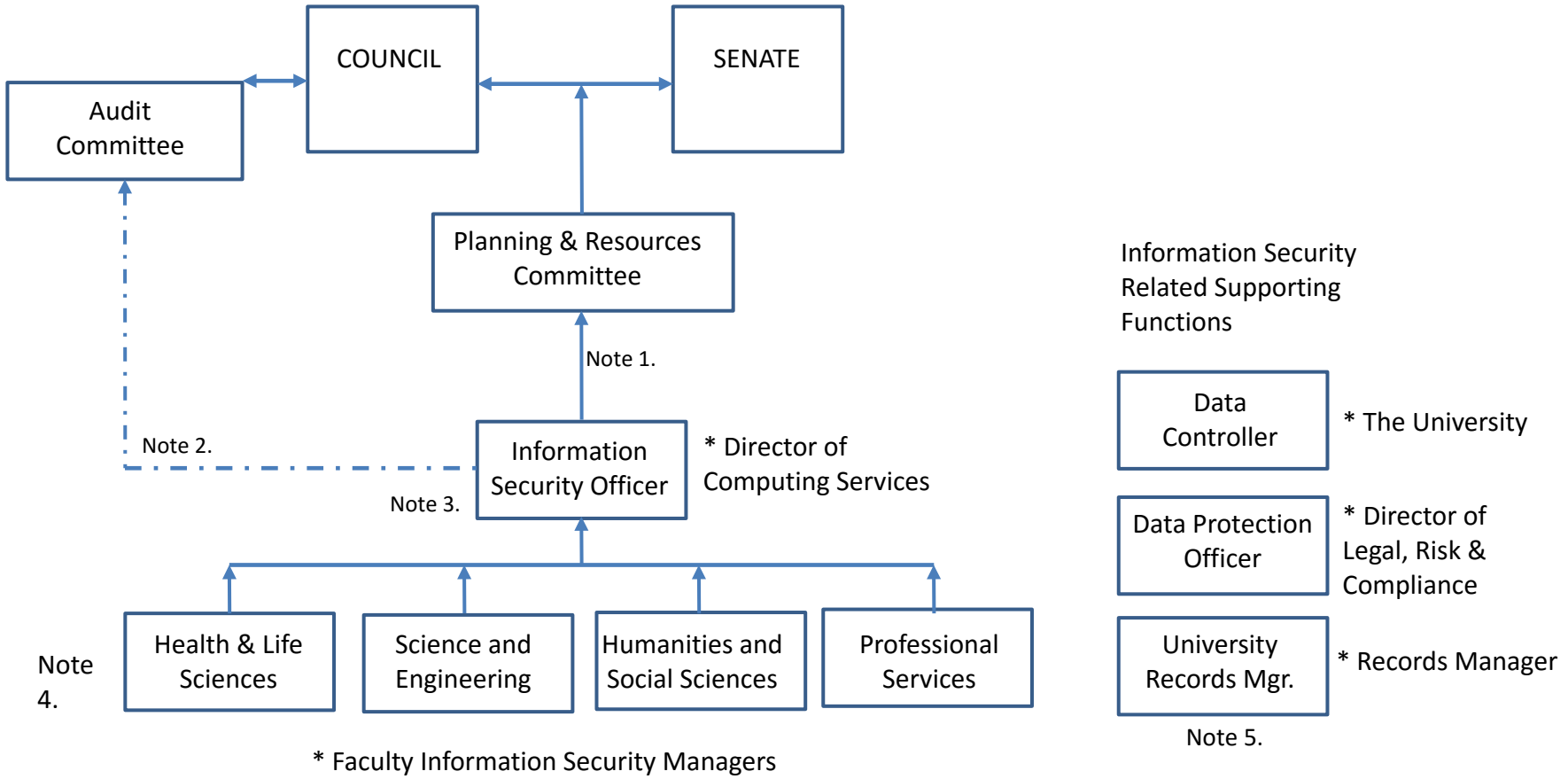
Users of laptop systems need to be particularly vigilant and take appropriate steps to ensure the physical security of the laptop system at all times, but particularly when travelling or working away from the University. Access to all laptop systems must always be controlled by the use of proper usernames and passwords. The policy on the use of laptops and mobile devices contains more information.

The policy on the use of laptops and mobile devices (see section 12) provides more details and guidance.

12. References

- An Introduction to ISO 27001: http://www.27000.org/iso-27001.htm
- University Data Protection policy: http://www.liv.ac.uk/legal/data_protection/policy.htm
- University Freedom of Information policy: http://www.liv.ac.uk/freedom-of-information/index.htm
- Regulations for the Use of IT Facilities at the University of Liverpool: http://www.liv.ac.uk/csd/regulations/regulations.htm
- Policy for the investigation of computers: http://www.liv.ac.uk/csd/regulations/investigationspolicy.pdf
- Policy on the use of laptops and mobile devices: http://www.liv.ac.uk/csd/regulations/codemobileandremote.pdf
- Records retention policy: http://www.liv.ac.uk/library/records-management/services/retention-schedule.html

Appendix A - Governance Framework



Notes:

1. Information Security Officer will report through the Chief Operating Officer
2. Relevant input to the Audit Committee regarding Information Security issues will be provided by the Information Security Officer
3. An Information Security Manager will be nominated within CSD to provide support to Faculty based Information Security Managers for day to day support and guidance for compliance, training and monitoring.
4. Information Security Managers will be nominated at Faculty level to ensure compliance with legislation and policy within the Faculty
5. Related Information Security functions will provide support in respect of legislations and policy.

Appendix B

Information Systems Security: Responsibilities for Heads of Departments

Background

This appendix describes the responsibilities of Heads of Departments for Information Systems Security in relation to computers in his/her area of responsibility.

- If all the computers in a department are connected to the Managed Windows Service (MWS) provided by the Computing Services Department (CSD) then no action is necessary.
- If a department connects any device to the University network, other than via a PC client service provided by CSD, then the Head of Department must appoint a system administrator and follow the instructions detailed in this policy document

Introduction

The University Network permits high-speed connection to the Internet from all connection points. This policy is for the guidance of all departments which run any computers which are networked but are not directly attached to the MWS (hereafter called connected local computers). The University network is operated so as to apply as few restrictions as practicable to the traffic between connected machines. This mode of operation is a fundamental part of a modern university computing service, but this freedom has associated risks that need to be addressed. Any machine or local network of machines connected independently to the University's data network is a potential security risk. To safeguard the University from major security breaches of its information systems, steps must be taken by each Head of Department to ensure that machines under their control (i.e. in their department but not connected to the MWS) are properly managed to minimise the risk. CSD will offer appropriate advice and support to assist with this.

General Policy

The following general policy statements apply to all computers in the University.

- Every computer connected to the University network must be subject to formal system administration. For computers attached to the MWS, this is undertaken by CSD.
- The University has formal Regulations covering the use and misuse of computing facilities. These formal regulations apply to departmentally administered machines as well as those managed by CSD. In the case of connected local computers the Head of Department acts, under delegated powers and with delegated responsibilities analogous to those of the Director of CSD in respect of CSD machines.
- CSD is able to provide advice on managing computers and users not administered by them. However, the owning department is entirely responsible for the maintenance of security on such computers.
- Responsibility for administration and security of computers must be assigned to a permanent member of staff who has been suitably trained and is technically competent. This role is known as the system-administrator. Postgraduate students do not meet these requirements and are therefore not suitable for this role.
- The staff members assigned the system-administrator role must have adequate time assigned to the function to enable them to maintain up-to-date security levels on the

computers under their control. Arrangements must be made to ensure the timely application of updates to maintain security whenever these are needed, and these arrangements must include the provision of cover for absence through holidays and sickness. This can be a non-trivial commitment, especially if the number of machines and users grows beyond one or two.

- CSD must be provided with a list of the names and contact details (phone numbers, email addresses, etc.) for all those who are responsible for system-administration of connected local computers. Departments are responsible for ensuring that CSD are provided with any changes to this list.
- Access to any local connected computer must be via a logon process that identifies and authenticates the user as authorised to use the facility in question. The only exceptions to this rule are the Library OPAC machines located in the Library buildings and which are restricted to OPAC access and a restricted set of electronic datasets only.
- Responsibility for maintenance and replacement of all departmental computers rests with the Head of Department.

System-administrator Responsibilities

Those staff designated to act as system-administrator for one or more computers should:

- Install and maintain the operating system and network connection environment in such a way that it is secure against unauthorised access either by users physically present at the main computer console or via the network connection.
- Monitor to a reasonable level the use of the computer so as to detect breaches of the system's security. In the event of a serious breach being detected, especially if network security may have been compromised, CSD should be alerted so institutional corrective measures can be taken.
- Implement and operate a user registration and authorisation scheme that permits authorised users to access the computer only as normal unprivileged users. CSD provides system-administration services for all machines directly managed by CSD staff. It also supports system-administration of many departmental machines that operate within the central University user Registration, Authentication and Authorisation scheme.
- All user names on departmental computers must be provided to CSD to enable such users to be traced.
- The only people who should be able to access the computers via the privileged root or administrator user names should be those appointed as system-administrators and these privileged user names should only be employed to perform system-administration tasks. Normal work even by the system-administrator should not be done under the privileged user names. Where a member of staff has the sole use of a single user machine they may (and the system may require this) operate that machine with administrator rights. Students should not be allowed access to computers via these privileged user names at any time.
- Ensure that each registered user is only allowed access to positively authorised facilities; the default on all computers should be to bar access.
- Monitor the availability of security patches and apply these whenever they become available. This will involve the continual observation of manufacturer and peer group email

lists, where the latest security information is exchanged and the timely implementation of the corrections distributed in this or other ways.

- Ensure that all software and/or data that are accessed via the computer are properly licensed for such access.
- Ensure by the establishment and operation of adequate backup procedures that all software and data stored on computers is secure against loss by accidental or deliberate system corruption.