

Information Security Procedures (2008)

1 Aims

- 1.1 The aim of this document is to establish clear procedures relating to information security.
- 1.2 All users of University IT facilities, whether staff, students or associates, are to comply with the Regulations for the Acceptable Use of University Information Technology ("the AUP"), the Information Security Policy and Procedures
- 1.3 It is University policy that all users of computing facilities at the University carry out their work in accordance with these procedures.
- 1.4 Where appropriate, compliance with the procedures will be monitored, and failure to comply may be subject to disciplinary action.

2 Acceptable behaviour

- 2.1 The AUP gives examples of acceptable and unacceptable behaviour in the use of IT facilities. All users must be aware of what is acceptable, and take individual responsibility for their actions.

3 Passwords

- 3.1 Appropriate usernames and passwords will be issued to all users. These will allow general access to IT facilities as well as individual access to specific corporate systems where required.
- 3.2 Each user has individual responsibility for the security of their password and it is forbidden to give a password to another person. Systems staff will never ask an individual to reveal their password.
- 3.3 Should the security of a password be compromised it is the responsibility of the individual user to change it and to establish that no breach of confidentiality has occurred. If there is a suspected breach of confidentiality this is to be reported immediately to the Help Desk.
- 3.4 Passwords chosen must be of sufficient complexity such that they are not easy for another person to deduce. In particular, for example, individuals should avoid choosing passwords that feature their name, partner's name, car registration, pet or anything that might be guessed or obtained by a third party.
- 3.5 Where technically possible, all information systems will enforce the following:
 - The minimum password length is six characters.
 - Passwords must be 'complex', that is consist of character(s) from at least THREE of the following four sets:

○ Lowercase letters	[a...z]
○ Uppercase letters	[A...Z]
○ Digits	[0...9]
○ Special characters	[` ! " £ \$ % ^ & * () - _ = + [] { } ; ' # : @ ~ \ , . / < > ?]

- Passwords will expire from time to time and at intervals less than 181 days.
- Previously used passwords cannot be re-used.
- Three logon attempts with incorrect passwords within 24 hours will lock an account.
- Locked accounts will remain locked until either:
 - a) reset by the Help Desk. The Help Desk will require adequate proof of identity prior to unlocking an account
 - b) unlocked by the user via a secure self service system
 - c) or after 24 hours the account will automatically unlock

3.6 If it is necessary to record a password it must be kept securely, disguised in some form.

3.7 In all cases, whether forced or not, passwords must be changed regularly – at least every 6 months.

3.8 In order to maintain user account security certain restrictions are in place to help prevent unauthorised access.

3.9 Some special non-user logon accounts may not have a password, for example 'projector' accounts, but these will be secured by other means, such as restricting their access and ability.

4 Training

4.1 All staff, students and associates will be offered appropriate training in the use of relevant IT facilities. All users must take individual responsibility for ensuring they are able to use correctly any information system to which they have been given access.

4.2 The University reserves the right to withdraw access to any system if an individual places the security of the University's systems or information at significant risk.

5 Information Security Officer

5.1 The University shall designate an individual as Information Security Officer, who shall be responsible for ensuring appropriate procedures, systems and guidelines are in place and implemented. Oversight of Information Security lies with the Information Systems Committee, and the Designated Authority as defined in the AUP.

6 Data Ownership

6.1 The Vice Chancellor has overall ownership of all University information, but delegates this responsibility to specific individuals ('information owners') responsible for identifying the use of that information. Individuals who create information will normally be deemed the owner of their own information or information that they have acquired. For information that applies to the corporate work of the University, this owner will normally be a manager.

6.2 All information held on university systems, including that held on n:\ drives and in email is owned by the University. All members of staff will have agreed to this when accepting employment at the University. Where there are concerns relating to intellectual property rights the individual must ensure the issue is specifically addressed in the employment contract.

7 Personal use

7.1 While the University does not provide data storage for personal use, it is accepted that limited personal use is allowed, as detailed in the AUP. However, University systems (including email), should not be generally used to store personal information.

- 7.2 Any personal information stored on your n:\ drive or in email is done so at the individual's risk. This data remains the property of the University. All data is regularly backed up and retained for at least one year, in order to protect the University from business loss in the event of systems failure.

8 Confidentiality

- 8.1 All corporate information should be kept confidential with computer screen's password protected and away from public view.
- 8.2 Individuals must always log out of a user session (or use the CTRL, ALT & DELETE keys to lock the screen when leaving a work station) and never leave a machine with a live connection to an information system.
- 8.3 Certain information is particularly confidential (e.g. exam scripts, marks, personal and medical data), and particular care must be taken with these¹. All users must be familiar with the University Data Protection Policy.

9 Legitimate use

- 9.1 Any use of University information must be lawful, honest and decent, and must pay attention to the rights and sensitivities of the people concerned.
- 9.2 The use of University information data for obscene, illegal or intimidatory purposes or which has the intent of annoying or offending somebody else is strictly forbidden.
- 9.3 University information and data may not be used for commercial gain.

10 Retention

- 10.1 Information must be kept only for as long as it is required, especially personal data. Certain categories of information must be legally retained for specified periods. All users must be aware of the retention periods detailed in the University Records Retention policy and ensure that they have processes in place to meet these.
- 10.2 All IT equipment must be disposed of in line with the WEEE regulations. In particular, any equipment or storage media which could contain any information or data must be disposed of in a secure manner. In general, all equipment should only be disposed of by or via the Computing Services department. CDs should be shredded.

11 Storage

- 11.1 Every member of the University is supplied with a networked default "Documents" store (N: drive). This is the usual place for storage of individual data. No information should be stored on local hard drives (C: drive). Where this is unavoidable (e.g. on a laptop being used remotely) information must be copied to networked storage as soon as possible.
- 11.2 Departments and teams are also provided with shared networked data storage. These areas should be used for all information which may be needed by more than one individual.
- 11.3 For portable temporary storage the use of USB memory sticks is recommended, but again, any information that is important must be copied to University network storage. Particular care must be taken to ensure the security of memory sticks.

¹ Policies and Procedures relating to the Conduct of Examinations, Preparation of Examination Papers, PPE5, Section 2

- 11.4 Data may be copied for use on a home computer, but the ownership will remain with the University. Any information modified on a home computer must be copied to networked storage as soon as possible. Data on home computers must be deleted as soon as it is no longer needed.
- 11.5 Any data relating to an identifiable living individual (and as such subject to the Data Protection Act) must not be stored on a laptop or removable memory or storage unless it is encrypted or otherwise secured (for instance through password protection). Where this is absolutely necessary, it should be stored for as short a period as necessary.
- 11.6 All University storage systems will have quotas in place, to prevent any individual abusing the system. These quotas will be as generous as possible, within current system constraints.

12 Access by others

Data stored in individual storage areas will not normally be accessed or made available to anyone else. However, this may be done in certain circumstances, either with or without the permission of the individual.

12.1 Access with your permission

- 12.1.1 Those who need to delegate responsibility for checking email to a colleague or assistant may do so through the "delegates" facility within Outlook. Having added the appropriate username as a delegate, various levels of permissions can be set for all aspects of Outlook including managing of both calendar functions and sending and checking of email.
- 12.1.2 More extensive delegation can be provided but this requires the account holder to apply by email to CS-liaison with details of to whom the account holder wishes to give full control of their email account (this can only be done for a member of staff or Outlook Exchange user).
- 12.1.3 Data, documents and files required by others should be saved to a departmental share drive – this will enable your team or department to share access to files. An individual may not grant access to their personal N: drive to anyone else.

12.2 Absence during employment

- 12.2.1 In the event of unplanned absence by a member of staff and access is required to information held only by that person, then in the first instance the staff member will be contacted and consent sought.
- 12.2.2 If consent is not or cannot be obtained, then a business case may be made by the Head of Department to the Assistant University Secretary to gain access to specific data on the n:\ drive or email. If the case is accepted, this will allow an authorised independent third party to search the absent member of staff's data or email for the specific information required which will then be passed to the Head of Department. Due to the administrative cost of this procedure, genuine business need must be proved.

12.3 Access without your knowledge/permission

- 12.3.1 The privacy of an individual's data and emails will normally be respected; however there are a number of situations in which access to data may be made
- Where a request is made under the provisions of relevant legislation in relation to the prevention or detection of crime, authorised staff may be requested to make an individual's data available
 - At the request of the data owner (the Vice Chancellor) or one of his named representatives
 - By Systems Administration Staff in connection with the maintenance of the systems

- Where an allegation or evidence of breach of the Regulations needs to be investigated, which will be carried out in accordance with the IT Investigation Policy.

12.4 After employment has ceased

- 12.4.1 Line managers are responsible for ensuring they have access to all necessary data before an employee leaves the University. It is necessary for an employee to make this data available by moving files to a shared drive or portable media device, on or before their last day at work; advice can be sought from the Help Desk
- 12.4.2 Where an individual requires assistance by Computing Services, written permission for data to be transferred to the network drive of a colleague or line manager must be given. These arrangements should normally be made at least one week before leaving the University.
- 12.4.3 An example of the permission document required is below:

“I hereby give permission for <named person> to have access to data on my n:\ drive and email after my departure from the university on <state date>. I understand that it is my responsibility to remove all personal data from both accounts before my departure, and that by arranging for this data to be passed to <named person> I am revoking any intellectual property rights.
I understand that after this data has been passed to <named person> both my network and email account will be deleted.
Signed <your signature>,
Name: <your name in full>,
Username: <your university username>”

Permission requests must be signed written originals; photocopies, faxes, or emails are not acceptable, nor is a letter signed as ‘pp’ acceptable for this purpose.

- 12.4.4 This permission will only refer to data available on the date of departure. It will not authorise the named person to access data previously deleted and stored on backup. Similarly it will not be possible to automatically redirect any future email to colleagues.
- 12.4.5 After departure, a vacation message can be set up on the email to inform people that you have left the University and provide an alternative address for contacts. This will allow the sender to email to the appropriate address; and will be displayed until the email account is deleted. During this time the email account will remain closed.
- 12.4.6 If you are concerned that you are the only contact for any business-related email then as soon as you are aware you will be leaving or moving jobs you should arrange for a business account or alias to be created by contacting the Help Desk, and inform all your contacts that this is the appropriate address to use.

13 System management

- 13.1 All of the University’s systems are to be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual system owners.
- 13.2 All systems management staff shall be given relevant training in information security issues.

14 Change Control

- 14.1 The implementation of new or upgraded software must be carefully planned and managed, to ensure that increased information security risks associated with any changes are mitigated.
- 14.2 There will be formal change control procedures, with audit trails for all changes to systems.

15 Access

- 15.1 Access to all information services shall use a secure logon process and access to high value systems may have further limitations as appropriate. Access will always be role/need and not by seniority of post.
- 15.2 Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained.
- 15.3 Access to IT systems is to be logged and monitored to identify potential misuse of systems or information.

16 Privileged Access

- 16.1 Certain members of staff will have elevated permissions on some or all systems. Some of these permissions are only granted when required but others will be granted implicitly by membership of certain domain groups.
- 16.2 A full charter expanding on these responsibilities is contained as Appendix A to this document.
- 16.3 With these elevated privileges comes increased responsibility, and all staff with elevated permissions will undergo training in their responsibilities. Abuse of privileged status will be regarded as a serious disciplinary matter.
- 16.4 If these staff leave the University, or are no longer a member of one of more of the membership groups, either through secondment or a permanent change in job role, these permissions will be revoked.
- 16.5 The University will regularly audit the status of all members of staff and accounts with increased privilege and confirm that this is still required and at the correct level.

17 Clocks

- 17.1 All System clocks will be regularly synchronised to the same time signal via automated processes such as NTP.

18 Capacity

- 18.1 Capacity demands of corporate systems shall be monitored, and actions taken to ensure increased demands are met. Users must be aware that disk storage and capacity is limited, and take reasonable care not to overload any system.
- 18.2 Any known or planned requirements for large amounts of storage or processing power must be notified to and agreed by the AUP Designated Authority well in advance.

19 Business Continuity

- 19.1 All corporate information systems and IT facilities will have a defined disaster recovery process in place. Systems designated as critical will have some level of resilience as long as this is technically possible and cost effective.
- 19.2 Responsibility for planning for being able to continue to operate without any IT facility is the responsibility of individual Heads of Departments. Full details are in the Business Continuity and Disaster Recovery Policy.

20 New information systems

- 20.1 The procurement or development of all new information systems must be discussed with the either the Head of Computing Services or Head of Corporate Information Services and approved by the Information Projects Programme Board.
- 20.2 Before introducing any new corporate data system, a risk assessment will include an assessment of any legal obligations that may potentially arise from the use of the system. The Head of Corporate Information Service oversees this risk assessment.

21 Misuse

- 21.1 If any member of the University knows of or suspects any misuse of IT facilities, they must report it either to their Head of Department or, if this is not appropriate, to the Head of Computing Services.
- 21.2 If the suspected misuse is by the Head of Computing Services, the matter must be reported to the Chair of the Information Services Committee or the Vice Chancellor.
- 21.3 In the case of reported or suspected misuse of computers or breach of the AUP by a student, then whatever the degree of reported or suspected misuse, the first response will be to disable the user's network and/or email account immediately. The purpose of this is to prevent any further misuse. At this time, the student's account history file will be checked to see if there is any record of a previous offence.
- 21.4 In accordance with the University's Student Disciplinary Procedures, Computing Services will in all cases refer the matter immediately to the student's Head of Department, with the relevant details. The Head of Department may meet with the Head of Computing Services or nominee to discuss the incident
- 21.5 As stated in the AUP, a breach of regulations may result in access to IT facilities being withdrawn, regardless of academic consequences.
- 21.6 In the case of reported or suspected misuse of computers or breach of the AUP by a member of University staff, the University Staff Disciplinary Procedures will be followed. Access to computing services may be withdrawn if appropriate.
- 21.7 In the case of reported or suspected misuse of computing services or breach of the AUP by guests or associates, computing access may be withdrawn pending investigation, and further action may include reporting the matter to the visitor's host department and/or home institution if appropriate.

Appendix A – Privileged User Charter

A.1. Introduction

System and network administrators, as part of their daily work, need to perform actions which may result in the disclosure of information held by other users in their files, or sent by users over communications networks. For these reasons they will have elevated and privileged permissions. This charter sets out the actions of this kind which authorised administrators may expect to perform on a routine basis, and the responsibilities which they bear to protect information belonging to others.

On occasion, administrators may need to take actions beyond those described in this charter. Some of these situations are noted in the charter itself. In all cases they must seek individual authorisation from the appropriate person in their organisation for the specific action they need to take. Such activities may well have legal implications for both the individual and the organisation, for example under the Data Protection and Human Rights Acts.

System and network administrators must always be aware that the privileges they are granted place them in a position of considerable trust. Any breach of that trust, by misusing privileges or failing to maintain a high professional standard, not only makes their suitability for the system administration role doubtful, but is likely to be considered by their employers as gross misconduct. Administrators must always work within the University's information security and data protection policies, and should seek at all time to follow professional codes of behaviour.

A.2. Authorisation and Authority

System and network administrators require formal authorisation from the "owners" of any equipment they are responsible for. The law refers to "the person with a right to control the operation or the use of the system". In the University this right is delegated by the Vice Chancellor to the Head of Computing Services and the Head of Corporate Information Services. This document will use the term "Designated Authority" which could refer to either of these posts, or other nominee, as is most appropriate.

If any administrator is ever unsure about the authority they are working under then they should stop and seek advice immediately, as otherwise there is a risk that their actions may be in breach of the law.

A.3. Permitted Activities

The duties of system administrators can be divided into two areas.

The first duty of an administrator is to ensure that networks, systems and services are available to users and that information is processed and transferred correctly, preserving its integrity. Here the administrator is acting to protect the operation of the systems for which they are responsible. For example investigating a denial of service attack or a defaced web server is an operational activity as is the investigation of crime.

Many administrators also play a part in monitoring compliance with policies which apply to the systems. For example some organisations may prohibit the sending or viewing of particular types of material; or may restrict access to certain external sites, or ban certain services from local systems or networks. The JANET Acceptable Use Policy prohibits certain uses of the network. In all of these cases the administrator is acting in support of policies, rather than protecting the operation of the system.

The law differentiates between operational and policy actions, for example in section 3(3) of the Regulation of Investigatory Powers Act 2000, so the administrator should be clear, before

undertaking any action, whether it is required as part of their operational or policy role. The two types of activity are dealt with separately in the following sections.

Operational activities

Where necessary to ensure the proper operation of networks or computer systems for which they are responsible, authorised administrators may:

- monitor and record traffic on those networks or display it in an appropriate form;
- examine any relevant files on those computers;
- rename any relevant files on those computers or change their access permissions
- create relevant new files on those computers.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, the administrator must not attempt to make the content readable without specific authorisation from the Designated Authority or the owner of the file.

The administrator must ensure that these activities do not result in the loss or destruction of information. If a change is made to user filestore then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

Policy activities

Administrators must not act to monitor or enforce policy unless they are sure that all reasonable efforts have been made to inform users both that such monitoring will be carried out and the policies to which it will apply. If this has not been done through a general notice to all users then before a file is examined, or a network communication monitored, individual permission must be obtained from all the owner(s) of files or all the parties involved in a network communication.

Provided administrators are satisfied that either a general notice has been given or specific permission granted, they may act as follows to support or enforce policy on computers and networks for which they are responsible:

- monitor and record traffic on those networks or display it in an appropriate form;
- examine any relevant files on those computers;
- rename any relevant files on those computers or change their access permissions or ownership (see Modification of Data below);
- create relevant new files on those computers.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it or by marking it as personal, the administrator must not examine or attempt to make the content readable without specific authorisation from the Designated Authority or the owner of the file.

The administrator must ensure that these activities do not result in the loss or destruction of information. If a change is made to user filestore then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

A.4. Disclosure of information

System and network administrators are required to respect the secrecy of files and correspondence.

During the course of their activities, administrators are likely to become aware of information which is held by, or concerns, other users. Any information obtained must be treated as confidential - it must neither be acted upon, nor disclosed to any other person unless this is required as part of a specific investigation:

- Information relating to the current investigation may be passed to managers or others involved in the investigation;
- Information that does not relate to the current investigation must only be disclosed if it is thought to indicate an operational problem, or a breach of local policy or the law, and then only to the Designated Authority (or, if this is not appropriate, to a senior manager of the organisation) for them to decide whether further investigation is necessary.

Administrators must be aware of the need to protect the privacy of personal data and sensitive personal data (within the meaning of the Data Protection Act 1998) that is stored on their systems. Such data may become known to authorised administrators during the course of their investigations. Particularly where this affects sensitive personal data, any unexpected disclosure should be reported to the relevant data controller.

A.5. Intentional Modification of Data

For both operational and policy reasons, it may be necessary for administrators to make changes to user files on computers for which they are responsible. Wherever possible this should be done in such a way that the information in the files is preserved:

- rename or move files, if necessary to a secure off-line archive, rather than deleting them;
- instead of editing a file, move it to a different location and create a new file in its place;
- remove information from public view by changing permissions (and if necessary ownership).

Where possible the permission of the owner of the file should be obtained before any change is made, but there may be urgent situations where this is not possible. In every case the user must be informed as soon as possible what change has been made and the reason for it.

The administrator may not, without specific individual authorisation from the appropriate authority, modify the contents of any file in such a way as to damage or destroy information.

A.6. Unintentional Modification of Data

Administrators must be aware of the unintended changes that their activities will make to systems and files. For example, listing the contents of a directory may well change the last accessed time of the directory and all the files it contains; other activities may well generate records in logfiles. This may destroy or at best confuse evidence that may be needed later in the investigation.

Where an investigation may result in disciplinary charges or legal action, great care must be taken to limit such unintended modifications as far as possible and to account for them. In such cases a detailed record should be kept of every command typed and action taken. If a case is likely to result in legal or disciplinary action, the evidence should first be preserved using accepted forensic techniques and any investigation performed on a second copy of this evidence.

Document control/change history				
Version	Author(s)	Date	Circulation	Comments
1	IE	April 2008	IS policy group	First draft from various sources
2	IE	August 2008	ISC policy T&F group, CS managers	Edited and completed, parts removed
3	IE/RM	Sept 08		Edit and tidy, plus appendix A
4	IE/RM	Oct 2008	ISC	final

Document approval and review	
Approved by:	Information Services Committee
Date approved:	
Review date:	
Author(s):	Ian Ellery
Owning Department:	Computing Services