

# 1 Corporate Information and Computing Services Continuity Plan

## Appendix 6: Code of Practice and related documents

This document provides a comprehensive guide to the University's policies relating to IT use and information handling, setting out both the formal University Regulations and a Code of Practice. It is the responsibility of all users of computing facilities, whether members of staff, students or others, to become familiar with the contents of this document.

### **Regulations on the Use of Computing Facilities**

#### **Code of Practice**

#### **Appendix 1 Additional advice**

#### **Appendix 2 JANET Acceptable Use Policy**

#### **Appendix 3 CHEST Code of Conduct for the Use of Software or Datasets**

### **Regulations on the use of Computing Facilities**

1. In these Regulations “computing facilities” means any computing facilities
  - (a) controlled by Corporate Information and Computing Services; or
  - (b) owned by the University or any University company; or
  - (c) situated on University premises;and “Head of Department” means the Head or Chairman of the Department which controls the facilities or the premises on which the facilities are situated.
2. No person may use computing facilities without the authorisation of the Director of Corporate Information and Computing Services acting on behalf of the Information Services Committee, or of the Head of Department or of the person or body to whom the facilities belong.
3. Every authorisation for the use of computing facilities shall be subject to the conditions that the facilities are to be used only by the person to whom the authorisation is given and only for the purpose or purposes for which it was granted and shall be subject to these Regulations.
4. Where the use of computing facilities is for the purposes of externally funded research or for purposes private to an individual user or external to the university, authorisation may be subject to the payment of charges prescribed from time to time by the Information Services Committee or by the Director of Corporate Information and Computing Services acting in accordance with any directions of that Committee.
5. No computing facilities may be used
  - (a) to secure unauthorised access to any program or data held in any computer wherever located;
  - (b) to cause any unauthorised modification of the contents of any computer, wherever located;
  - (c) in any way which jeopardises the work of others, or the integrity of the equipment or of any programs or data; or

(d) in breach of the Computer Misuse Act 1990 or other applicable legislation, or of any local rules made by the Director of Corporate Information and Computing Services or the Head of Department.

6. No student or member of the University staff may use any means

(a) to secure unauthorised access to any program or data held in any computer facilities; or

(b) to cause any unauthorised modification of any such material.

7. Any breach of these Regulations may be dealt with, in the case of students under the Discipline Regulations and in the case of members of the staff of the University in accordance with disciplinary procedures approved (subject to the Statutes) by the Council. Any person suspected of a breach of these Regulations may be debarred from access to computing facilities by the Director of Corporate Information and Computing Services or the Head of Department until the appropriate disciplinary procedures have been completed; any use or attempted use of facilities by a person so debarred from access or by another acting on that person's behalf shall constitute a breach of these Regulations.

Note: These Regulations should be read in conjunction with the Code of Practice for the Use of University Computing Facilities.

## 2 Code of Practice

Throughout this document, reference to any computing equipment, facilities or resources means any computing facilities: controlled by the University's CICS; or owned by the University or by any University company; or situated on University premises [see [Regulation 1](#)]. It also covers information stored on the campus network, the campus management and administrative computing facilities, networked and standalone personal computers on campus, and any facilities used for processing such information off campus (including laptop machines and home-based facilities). The University of Sheffield has a dynamic IT environment, characterised by the free sharing of information. The purpose of this Code of Practice is not to restrict the general openness experienced in a creative institution, but merely to safeguard certain essential activities of the University.

### Access to facilities

The use of computing facilities requires authorisation in accordance with [Regulations 2, 3 and 4](#). Prior permission must be obtained from CICS before any machine (PC, printer, etc.) can be connected to the network.

### Storage and publication of information

Users must recognise that the resources of the University's network are limited and take due account of this in any use of the system. This consideration is relevant to the volume and nature of electronic mail, to individuals, news groups, and mailing lists; the size and location (particularly in other countries) of any files to be transferred; the use of programs that check for new files or logins every few seconds; and the storage of large amounts of data on central file servers. The University is now charged by usage for certain network facilities, including a large proportion of incoming transatlantic traffic.

### Data protection

Where personal data is to be stored, a user must comply with the Data Protection Act 1998.

The Data Protection Act 1998 concerns information about living, identifiable individuals that is processed automatically, or held in structured manual files. The Act gives individuals the right to have access to information stored about them and requires that this information is maintained and is correct. Organisations holding personal data must be registered with the Data Protection Registrar (an independent officer who reports directly to Parliament).

In addition, data users must comply with eight Data Protection Principles established by the Act. The Data Protection Principles are intended to protect the rights of the individuals about whom personal data is recorded. Guidance as to compliance with the principles may be obtained from the University's Data Protection Officer.

A user must ensure that the use of University-related personal data is restricted to the minimum consistent with the achievement of academic purposes; and contact the University's Data Protection Officer before conducting any activity that involves any form of processing of personal data.

## **Publication of information**

The dissemination of information through the University's network or the Internet is in law the 'publication' of that information, and all legal rules governing publication (for example as to defamation) apply. Similarly, publication may have other legal effects; it may, for example, bar a subsequent application for a patent.

No user may create, store, exchange, display, print, publicise or circulate offensive or illegal material in any form, this includes:

any material that is pornographic, excessively violent or which comes with the provisions of the Obscene Publications Act 1959 or the Protection of Children Act 1978 (Any such publication will be regarded as a very serious matter, which will be reported to the police);

any material which may encourage discrimination on grounds of sex, gender, sexual orientation, race or ethnic origin, or which would contravene the Sex Discrimination Act 1975 or the Race Relations Act 1976; particular care is needed in the advertising of posts;

any material in the form of an advertisement (even in specific Usenet newsgroups) which does not comply with the Code of Practice issued by the Advertising Standards Authority, requiring that all advertisements should be "legal, decent, truthful and honest".

Users must not use the computing facilities to originate or forward chain letters, "for-profit" messages, or for the purposes of a pyramid selling scheme.

## **Copyright material**

A user must not copy any copyright material without the written permission of the owner of the copyright, unless copying is covered by some other provision such as that in a software licence. The University reserves its rights to the crest and logos which are its property; they, and departmental addresses, may be used only for official purposes.

## **Electronic mail**

A user is responsible for all electronic mail sent from his or her account. Care should be taken to ensure that e-mail is sent only to the intended recipients and the content of messages should be checked before sending. It should be considered that e-mail may not be the best medium for sensitive information. A user must avoid careless or excessive use of e-mail as this may slow or restrict network access. It is prohibited to forge (or attempt to forge) e-mail messages, or to read, delete, copy, or modify the electronic mail of other users.

Electronic mail can be forged. A user who suspects that a message may not have been sent by the apparent originator should reply (or telephone) and ask for confirmation. Any misuse of electronic mail should be reported to CICS and will be investigated.

## **Misuse of facilities**

[Regulation 5](#) prohibits the misuse of computing facilities. No user may seek to or secure unauthorised access to any program or data held in any computer wherever located ([Regulation 5a](#)); a user must not attempt to decrypt system or user passwords or copy system files.

No user may use computing facilities so as to cause any unauthorised modification of the contents of any computer, wherever located, or in any way which jeopardises the work of others, or the integrity of the equipment or of any programs or data

([Regulation 5b,c](#)). This prohibits, inter alia, unsolicited or unauthorised "security tests" or "recovery tests", and the introduction of any viruses, worms, Trojan horses, logic bombs or any other harmful, disruptive, destructive or nuisance program or file on to any of the computing equipment, nor take action to bypass any security precautions installed by an appropriate authority to prevent this. (Further information on viruses is given in [Appendix 1](#)).

Careful consideration should be given to the content of any published material (eg e-mail, newsgroup contribution, Web page, images displayed on a screen, computer printout). Material that is unacceptable to the recipient and which creates an intimidating, hostile or offensive environment may constitute harassment under the University's guidelines. Publication of such material outside the University may harm the University's good name.

Users of University IT facilities must conform to all applicable rules of English law, for example the laws on pornography, blasphemy, and financial services advice.

The Computer Misuse Act 1990 creates a number of criminal offences:

Unauthorised access to computer material ('hacking') including the illicit copying of software held in any computer. This carries a penalty of up to six months imprisonment or up to a £5000 fine.

Unauthorised access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking, with a penalty of up to five years imprisonment and an unlimited fine.

Unauthorised modification of computer material, which includes the intentional and unauthorised destruction of software or data; the circulation of "infected" materials on-line; and the unauthorised addition of a password to a data file. This offence also carries a penalty of up to five years imprisonment and an unlimited fine.

## **Discipline**

Breach of the Regulations is dealt with under [Regulation 7](#). In addition, use of computing facilities in breach of this Code of Practice may lead to the restriction of access to or the withdrawal of computing facilities.

Any use or attempted use of facilities by a person debarred from access or by another person acting on that person's behalf constitutes unauthorised use is therefore a breach of the [Regulations](#).

## **Use of Open Access Areas**

University open access computing facilities must be used solely for study related purposes between the hours of 9:00 a.m. and 5:00 p.m., or at other times if there are no machines free for academic work. Social e-mail, Internet chat and Web access for leisure are unacceptable when others are waiting to work. Misuse should be brought to the attention of CICS, with details of the machine used, the date and time.

Disciplinary action will be taken where appropriate.

Logged in machines should not be left unattended in open access areas. Only one machine can be used by any individual at a given time. It is not permitted to reserve machines, either physically or by any other means (for example, running a password protected screen saver). Any other individuals who require the use of such a machine are within their rights to reboot and use that machine.

Food and drink is not permitted in any open access facility, and smoking, as within any other part of the University buildings, is prohibited. Noise should be kept to a minimum to encourage a good working environment. Threatening, harassing or abusive behaviour directed towards staff or fellow users is unacceptable. Offensive material (abusive, sexist, racist, or pornographic) may not be displayed or printed in an open access area.

### **Physical Precautions**

All proper precautions should be taken to protect the physical security of equipment and information. Use of physical security devices (such as clamps to secure computer processor units to desks) is recommended on all system equipment. Evidence of recently purchased equipment (for example, packing cases) should not be left on view for potential thieves to see.

Sensitive information can often be left in a vulnerable state merely by others gaining physical access. Office doors should be kept locked when the occupant is away and where this does not conflict with safety regulations. Computer display screens and printers should be positioned strategically to avoid accidental disclosure of sensitive material. A user should always log off from the computer account if leaving the computer unattended.

As private information is only as secure as the security mechanisms employed on the system on which it is maintained, sensitive, and particularly clinical data, should where possible be maintained on a secure stand alone machine. When sensitive information is stored on a backup medium, precautions must be taken to ensure the storage is secure. Particular care should be taken to ensure physical security.

If sensitive information is processed off-campus, the same stringent procedures must be applied as on-campus. Machine access should be restricted and secure.

When transporting or transferring information, the information on separate media (e.g. floppy disk, tape, zip disk, etc.) should where possible be kept away from the hardware, to reduce the risk of theft. Hardware or media should not be left unattended when travelling; portable computers should be carried as hand luggage.

Access to sensitive information should be strictly controlled when temporary staff or students are employed. Students should not have access to information stored about other students.

### **Passwords**

The password to a user's account is the key to the security of information, and more generally the integrity of the network system. A user is responsible for all activities and possible misuse originating from his or her account, and it is important that the password is not disclosed to anyone, whether intentionally or accidentally. It should not be written down or permanently stored on a machine or in a database. If a problem arises with a user's account, the password may be disclosed to a recognised member of CICS; the password should be changed immediately after any such disclosure. (Advice on passwords is given in [Appendix 1.](#))

### **Software Licences**

Users must comply with the terms of software licence agreements, copyright and contracts. A user is responsible for ensuring that his or her use of software is covered by a current licence or contract. Software provided on servers and central systems, including site licensed and Microsoft licensed software, must not be copied to hard

disk or anywhere else. Software with non-transferrable licences must be removed when machines are decommissioned.

Similarly, use of facilities provided through JANET and CHEST and similar organisations or networks must comply with the relevant conditions and policies (see Appendices 2 and 3).

### **Departmental records**

Every department should

- a. maintain a complete register of equipment including memory and hard disk capacities, and of all software installed on machines in that department
- b. keep all software licences securely locked in a departmental office.
- c. log and report to CICS all security incidents or suspected incidents and ensure they are investigated.

Appropriate information should be provided to insurers to ensure that they are aware of any changes in the risk covered.

### **Equipment Decommissioning**

When equipment is no longer of use it must be fully decommissioned. Software with non-transferrable licences must be removed. Machines that have been used to store sensitive information must have a low level initialisation performed on their hard disk, as deleting files merely removes the index to data stored and information might still be retained on the disk. Particular vigilance should be observed when removing passwords, personal information, etc. from hard disks. Further information regarding decommissioning of hardware is available by contacting CICS.

Staff who are leaving a department to work elsewhere in the University should re-register and have their old account disabled once any relevant files have been transferred. Staff who are leaving the University must inform CICS so that their account can be disabled. If a staff member leaves, or is absent from the University for a time, and his or her account has specific access right to systems or functions that are required by a department, the rights should be transferred to another member of staff rather than the absent staff member's account being used.

### **University liability**

The University can accept no responsibility for the malfunctioning of any computing facility, loss of data, or the failure of any computer security system, or any losses while using University systems. The University does not guarantee the continued availability of any IT facilities and accepts no liability for any loss or damage caused by the temporary or permanent withdrawal thereof.

### **3 Additional advice**

#### **Viruses**

A computer virus is a malicious parasite program written to alter the way your system operates without your permission or knowledge. It may destroy data, display messages or destroy functionality. A virus spreads by copying itself to other disks as they are loaded on an infected system. They are primarily a problem when floppy disks are exchanged by users. The virus is propagated to new systems if it is booted from, or runs a program from, an infected disk. However, they are becoming more and more sophisticated. It is not only floppy disks that can be infected, fixed disks and network disks can also be compromised.

The basis of protection is awareness of the dangers of using external disks that may be infected and the use of appropriate virus detection software. Users are advised not to run or load any files into a system unless they come from a recognised and reliable source, which does not necessarily include all software providers. System software running across the network is regularly checked for viruses and is highly secure.

Virus check all floppy disks of uncertain or external origin before use. Public domain (freeware) and shareware software, probably obtained from the Internet, and any demonstration software from manufacturers should also be virus checked before use. The University operates a suite of market leading anti-virus software for all hardware system types used on campus. The software is updated every month to take account of the ever increasing number of viruses. It can be used from the network or via floppy disk, which can be obtained from the IT Centres or Computer Centre.

#### **The choice of a password**

Some passwords (names or words in the dictionary) can easily be broken using public domain software, others (car registration or telephone numbers) are easily guessed. Hence, never use a password that originates from your name, your partner's name, the name of your pet, etc.

Other techniques that are commonly thought to be secure but are not are the use of reversal and appending. Memorable words (or names) are just reversed by the individual or repeated. Again password cracking software can easily check for such ruses. So for example, do not use "egroeg" (the reversal of george) or "georgegeorge" (the appending of george to itself) or "georgeegroeg" (a reversal appending combination).

Similarly it is not secure to simply use your username (or the reversal) also as your password.

Passwords should be alphanumeric (i.e. combinations of both letters and numbers). However, it is not a case of just appending or prepending a number onto an otherwise easily guessed password. Hence, for example do not use "john3" or "7susan". Also do not convert standard letters into numbers, for example replacing the letter "1" with the number "1" or the letter "o" with the number "0". So do not use something like "he110".

Punctuation characters ( , . ; : ? ) and mixed case combination passwords can also be used with some systems. (Upper and lower case letters are not differentiated on a Novell system i.e. a password for a network PC account is case insensitive.)

A password should consist of 7 characters or greater.

A good system to use when choosing a password is to think of a phrase that is memorable to you, then break this down to the first character of each word, and

finally intersperse this with a few numbers and punctuation. So for example, using the phrase "the geese fly backwards over Sheffield" you would break this down to "tgfbos" and then mix in some numbers and punctuation to end with a password of "t3gf4b:os". Be wary, however, of using well-known phrases like quotations from Shakespeare ("tbonbtitq"). In addition, you should also think about how fast you can type a more difficult letter combination password, particularly in the presence of others who may be able to observe and remember a slowly typed password. Another approach can be to use combinations of memorable personal information interspersed with enough static. For example, someone with a birth date of 12 October 1976 may combine some of this information into a password like "Oc?to12b.76". Those with system rights access should be more careful about their choice of password and the regularity that the password is changed.

### **Backups and Storage**

It is recommended that, in the majority of cases, information be copied regularly to backup media (e.g. floppy disk, tape, zip drive, etc.). It is also recommended that backup media are stored away from the equipment they protect, in case of machine failure, fire or catastrophe. Computers are machines and all machines will fail at some point.

In addition, you are advised to abide by the following:

save your work regularly as you are working;

always save into your network account (drive U:) or onto your hard disk;

NEVER save directly onto a floppy disk (drive A:);

periodically close down the software and COPY important saved files onto a floppy disk.

In the event of server failure, people who had followed the above steps would be in a position to use an alternative machine, or a different server as a guest, with a recent copy of their work on floppy disk.

There are, however, exceptions to the copying of information. Information obtained from the central MIS systems should not be stored as a backup. Such a procedure would only present a further unnecessary security risk. Local copies of information from central databases should not be made; this could lead to the carrying of out-of-date information, or more seriously could be a breach of the Data Protection Act.

## 4 JANET Acceptable Use Policy

JANET is the network that links Universities, Colleges and research organisations throughout Great Britain and Northern Ireland. There are direct links to networks in Europe and the USA, by which JANET forms part of the global Internet. JANET is maintained to support teaching, learning and research. If a user sends or receives e-mail off-campus, use the World Wide Web, or any other Internet facilities this involves utilising the JANET network.

The following are extracts from the JANET acceptable use policy (Version 4, April 1995) available for fuller consultation on the Web at

<http://www.ja.net/documents/use.html>

Subject to the following paragraphs, JANET may be used for any legal activity that is in furtherance of the aims and policies of the User Organisation.

JANET may not be used for any of the following.

1. The creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
3. The creation or transmission of defamatory material;
4. The transmission of material such that this infringes the copyright of another person;
5. The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks;
6. Deliberate unauthorised access to facilities or services accessible via JANET;
7. Deliberate activities with any of the following characteristics:
  - wasting staff effort or networked resources, including time on end systems accessible via JANET and the effort of staff involved in the support of those systems;
  - corrupting or destroying other users' data;
  - violating the privacy of other users;
  - disrupting the work of other users;
  - using JANET in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
  - continuing to use an item of networking software or hardware after UKERNA has requested that use cease because it is causing disruption to the correct functioning of JANET;
  - other misuse of JANET or networked resources, such as the

introduction of "viruses".

8. Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET.
9. Where violation of these conditions is illegal or unlawful, or results in loss or damage to UKERNA or JANET resources or the resources of third parties accessible via JANET, the matter may be referred for legal action.
10. It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of JANET resources on the part of users and appropriate disciplinary measures taken by their Organisations.

## **5 CHEST Code of Conduct for the Use of Software or Datasets**

The operation of software obtained from/via CHEST (Combined Higher Education Software Team) must conform to the CHEST terms and conditions; such software is licensed for University use only. Because CHEST negotiated software originates from many different sources, the licensing associated with the software will vary. The CHEST Code of Conduct for the use of Software or Datasets, set out below and to which University users must conform, has been endorsed by FAST (Federation Against Software Theft) and is available for viewing on the Web at <http://www.chest.ac.uk/conduct.html>

This Code of Conduct should be observed by all users of software and/or computer readable datasets, hereafter referred to as "Product", that has been issued or made available to them by the "Institution". This Code does not constitute a licence and, in all cases, users of Product should acquaint themselves with the provisions of the relevant licence when they obtain a copy and before putting the same to use.

The Code of Conduct is in three parts :

- a. The Code
- b. Definition of Educational Use
- c. Copyright Acknowledgement

### **a. The Code**

Unless advised to the contrary it is to be assumed that Product is subject to Copyright Law and is provided for Educational Use, see "Definition of Educational Use".

The Institution will maintain a record, or require any Department which is in receipt of Product to maintain such a record, of each Product that is available for use in the Institution or, in the case of devolved responsibility, within the Department. In either case the record shall contain details of the licensing arrangements for each Product together with the names of any persons to whom a copy has been issued.

All employees and students of the Institution will be informed of this Code of Conduct and all users of Product will be advised of the conditions under which it may be used and will sign that they have been so advised. In the event that users, who are neither employees or students of the Institution, are authorised access to Product they will be similarly advised and shall be required to sign that they have been so advised and will further sign that they will abide by the Code before being given access to Product. The responsibility for ensuring that such users are so informed may be devolved to the "home" Institution by prior agreement between the Institutions. All employees and students of the Institution will be issued with a copy of the Copyright Acknowledgement.

The Institution will organise arrangements for back-up, copying and distribution of Product and Documentation subject to the conditions of the licence. Users shall not copy or distribute copies of the software unless permitted to do so under the terms of the licence.

Where it is a condition of supply of Product the Institution will organise a single point of contact for dealing with queries and support of Product. It is recommended that, unless special conditions pertain, this point of contact should be within the Computer Centre.

In the event of termination of the licence for a Product, the Institution will instruct the single point of contact to call in all copies of Product and, where appropriate, make arrangements for the safeguarding of the authorised archival copy.

The Institution shall not permit users to reverse engineer or decompile Products unless permitted so to do under the terms of the Copyright, Designs and Patents Act 1988 and associated Statutory Instruments, or under the terms the licence.

The Institution will use its best endeavours to apply, administer and ensure compliance with this Code of Conduct.

## **b. Definition of Educational Use**

### **Note 1**

The following are the ground rules and any variation should be a matter for discussion either centrally, by the body negotiating the licence terms, or, where there is no community-wide negotiation, by an Institution BEFORE the form of licence is signed.

### **Note 2**

The following is a full quotation from the "General Licence Conditions" which apply in CHEST centrally negotiated agreements and in the recommended "Form of Licence" for non-centrally negotiated offers.

Product may be used by any employee, student, or other persons authorised by the Licensee for the purposes of the normal business of the Licensee's organisation, whether or not they are located on the Licensee's premises. Such use of Product includes the following:

- a. Teaching
- b. Research
- c. Personal educational development
- d. Administration and management of the business of the Licensee's organisation.
- e. Development work associated with any of the above.

General Exclusions:

- i. Consultancy or services leading to commercial exploitation of Product
- ii. Work of direct benefit to the employer of students on industrial placement or part-time courses paid for by the student's employer.

In (i) and (ii) above the Licensor may allow such use in return for acknowledgement of use of Product and/or for an agreed fee.

**Note** "Commercial Exploitation" in the context of this Code is the use of Product for monetary gain either by the Institution or an individual. Where Product is so used this must be a matter for discussion between the Supplier and the Licensee.

No persons shall be excluded from use of Product for reasons of nationality or citizenship.

All persons who are provided by the licensee with copies of Product must have signed a declaration incorporating the Copyright Acknowledgement.

### **c. Copyright Acknowledgement**

I agree that my usage of any Software or Computer Readable Datasets, hereafter referred to as "Product", issued or otherwise made available to me by a School or Department of an Institution is subject to the following conditions:

0. I will ensure that all the requirements of the agreements or contracts under which Product is held by the Institution will be maintained. (Copies of the relevant agreements or contracts may be seen by application to the School or Department which made Product available.)
1. I will not remove or alter the Copyright Statement on any copies of Product used by me.
2. I will ensure the Security and Confidentiality of any copy released to me, and will not make any further copies from it or knowingly permit others to do so.
3. I will use Product only for purposes defined in the Agreement, and only on computer systems covered by the Agreement.
4. I will not incorporate a modified version of Product in any program written by me without express permission of the Licensor.
5. I will not reverse engineer or decompile Product or attempt so to do other than as provided for by the terms of the Copyright, Designs and Patents Act 1988 and associated Statutory Instruments, and after confirmation of such permission from my Institution.
6. I will return all copies of Product at the end of the course/year/period of employment or when requested to do so.

In signing this Copyright Acknowledgement, I realise that the Institution reserves its right to take legal action against individuals who cause it to be involved in legal proceedings, as a result of violation of its licensing agreements.