Computing & Media Services (C&MS)

ICT Usage: Code of Practice for students

In order to provide our users with a safe, reliable and resilient computing environment it is necessary for us to set certain conditions on its use. These conditions are not unduly onerous and shouldn't prevent anyone from doing what they need to do. However it is important that all users comply with these conditions and use of our facilities implies acceptance of these conditions. Failure to comply renders the offender liable to sanctions and or disciplinary action.

Information Technology and Computing at Marjon

The University provides IT and computing facilities for use by all its students. Almost all students are likely to use Information Technology as part of their taught course or project work. To help you get started we have produced this guide showing what resources we have, how you can access them, what your responsibilities are and what to do if you have a problem.

Remember, we are here to help you and we welcome any and all feedback to help us improve our service to you.

What IT resources are there?

The vast majority of PCs are connected to the University network and from any networked PC you can access a range of application software (Word, Excel, Access, Email and a variety of graphics, statistics and other programs) and all networked PCs have access to the Internet.

How do I access these resources?

To gain access to these resources you will need to logon to the network. As a student **your username is your unique 8 digit student ref number which is printed on your ENROLMENT FORM**, your initial password will be Marjon-ddmmyyyy (where ddmmyyyy is your birth date in number only format) and you should change that password for one of your own choosing once you have logged on. You will be provided with an area of network space where you can save your work, this workspace is limited and you will need to regularly delete old files. If you find this space is too little for the demands of your course please speak with your course tutor who will request an increase from C&MS (please remember that network disc space is a finite resource and it is not possible for us to simply give every student unlimited space). The present standard quota limits for students are 500Mb of network space

Whilst the University makes every effort to maintain secure backups of all student created data stored on the network it cannot guarantee the availability of that data under any and all circumstances. It is ultimately the student's responsibility to ensure that they have secure copies of their own data.

What about printing?

You can print to any of the network-connected printers. Each print request will be debited from your printer credits account when you release the job at the printer. You can top up your printer credits by purchasing print credits from either the campus shop or the library.

What are my responsibilities when using IT at Marjon?

Code of Practice

Throughout this document, reference to any computing equipment, facilities or resources means any computing facilities: controlled by the University or owned by the University; or situated on University premises. 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 St Mark & St John 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, prior permission must be obtained from C&MS 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.

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.

There may be some occasions where the creation, storage and exchange of data of an offensive nature may be justified in the context of learning, teaching and / or research. In such circumstance permission from the Deputy Vice Chancellor & DCE must be given in advance.

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 C&MS and will be investigated.

Misuse of facilities

The University 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; 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. 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 the University’s disciplinary procedures. 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 Code.

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 C&MS, 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.

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 C&MS; 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).

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.

Monitoring

No expectation of privacy should be taken with regard to the use of the telephone, voice-mail and ICT systems. Users should be aware that telephone use, voice-mail boxes and ICT use is monitored in accordance with this policy.

Appendix 1 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 removable 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 removable 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 removable 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 uses industry standard anti-virus software which is regularly updated to take account of the ever increasing number of viruses

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 "l" with the number "1" or the letter "o" with the number "0". So do not use something like "he110".

A Marjon password will consist of 14 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 University of St Mark & St John" you would break this down to "tgfbouosmasj" and then mix in some numbers to end with a password of "t3gf4b5ocosmasj". Be wary, however, of using well-known phases like quotations from Shakespeare ("tbontbtitq"). 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.

Backups and Storage

It is recommended that, in the majority of cases, information be copied regularly to backup media (e.g., CDRW, pen drives 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 explicitly save into your network account;

Periodically close down the software and COPY important saved files onto a CD, DVD or pen drive.

Use of Display Screen Equipment

No matter how good your typing skills (or lack of them), you can suffer serious ill effects if you use display screen equipment without a few sensible precautions.

1. Make sure that your equipment is properly adjusted

Ensure that your lower back is well-supported by adjusting the seat back height.

Adjust your chair seat height so that your forearms are level when using the keyboard.

Make sure that the leading edge of the keyboard is at least 8-10 cm away from the edge of then desk.

If you use a mouse, have it far enough away from the edge of the desk so that your wrist is supported whilst you use it. If you can learn to use the mouse with either hand, so much the better.

2. Do not have your screen positioned in such a way that there is glare from the windows or room lights.

3. Maintain good posture - do not lean to one side or the other.

4. Take regular breaks away from display screen work. The experts recommend that you should take at least 10 minutes off every hour. Most departments will have a Display Screen Trainer and/or Assessor who will be able to offer you specific advice if you use a display screen on a regular basis.
More information on working with VDU's can be found at the Health and Safety Executive Web site.

Appendix 2 JANET Acceptable Use Policy

JANET is the network that links Universities, University 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 **www.ja.net**
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.
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;
The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
The creation or transmission of defamatory material;
The transmission of material such that this infringes the copyright of another person;
The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks;
Deliberate unauthorised access to facilities or services accessible via JANET;
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".
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.
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.
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.

Appendix 3 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 :

The Code

Definition of Educational Use

Copyright Acknowledgement

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 nor 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.

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:

Teaching

Research

Personal educational development

Administration and management of the business of the Licensee's organisation.

Development work associated with any of the above.

General Exclusions:

Consultancy or services leading to commercial exploitation of Product

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.

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:

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.)

I will not remove or alter the Copyright Statement on any copies of Product used by me.

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.

I will use Product only for purposes defined in the Agreement, and only on computer systems covered by the Agreement.

I will not incorporate a modified version of Product in any program written by me without express permission of the Licensor.

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.

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.

CONTACTS:
C&MS
Web: **http://helpdesk**
Email: **computingservices@marjon.ac.uk**
Phone: x4333
Pop in and see us in 24 hour Open access room by the library

Document title:	ICT Code of Practice for students
Document reference:	ICT Code of Practice for students
Author:	David Riggs
Document date:	1st March 2005
Date last amended:	8th October 2013
Confidential?	No
Document status:	Draft
Document Version:	0.5
Circulation:	Open
EIA	Carried out 25th June 2009
History:	Amended for University status Oct 2013 Amended to make student specific. 16th June 2009