

Rules for the use of University Computers and Data Networks

1. Introduction

1.1 Scope of these Rules

These rules are, in part, derived from the Universities and Colleges Information Systems Association (UCISA) Model Regulations. They apply to all Information Technology (IT) facilities provided by the University, connected to the University's network or used on the University's premises. These conditions apply to all users of such facilities and all types of usage; they also apply to the use of the Joint Academic NETwork (JANET) and to the use of any remote devices whether accessed via JANET or otherwise, including access via personally-owned devices.

Users are responsible for ensuring that they are familiar with these rules and any specific rules that apply to particular systems. Parts 4 and 5 below relate specifically to facilities provided by IT Services.

Users must ensure they comply with the University's policies and sub-policies on Information Security and, where applicable to their role, University policies relating to systems and network management. These are all available from www.reading.ac.uk/information-security.

1.2 Disciplinary Action

Users who breach these conditions may first be warned of their unacceptable use. Failure to respond to a warning, repeated breaches or serious transgression will result in immediate withdrawal of access to computing facilities. Violation of these conditions may be dealt with through the University's disciplinary procedures set out in Ordinance XVII and in the Regulations for Conduct. Legal action may be taken by the University where appropriate.

2. Legal Requirements

Infringements of the civil or criminal law are subject to penalties including fines and imprisonment and the University may refer such infringements for legal action. Such infringements may also incur University disciplinary action.

The following acts are relevant to computer use. The examples given below are intended as a guide and do not attempt to cover all eventualities.

2.1 Computer Misuse Act 1990

This act specifies three offences:

2.1.1 *Unauthorised access*

Examples would include using another user's username and password for any reason with or without their agreement; attempting to access another user's files without their express permission; impersonation via e-mail, news, web or other service. Sharing a username and password on the University system, without explicit arrangement with IT Services, constitutes an offence by both lender and borrower.

2.1.2 Unauthorised access with intent

Examples would include accessing financial, administrative or examination data without authorisation.

2.1.3 Unauthorised modification

Examples would include destroying another user's files, creation or introduction of a virus, changing examination results or deliberately generating information to cause a system malfunction.

2.2 Copyright, Designs & Patents Act 1988

All software (including computer programs) accessible via the network and installed locally on University machines is protected by copyright and therefore subject to restrictions on its use. Users must comply with the terms and conditions of software licence agreements and abide by policies for acceptable use.

No unauthorised copying of software is permitted except as where expressly stated within the terms of the licence.

Users must treat as privileged any information not provided or generated by themselves that may become available to them through their use of computing facilities; no part of such information may be copied, modified, disseminated or used without the permission of the appropriate person or body.

Users installing software and information on University equipment (including remote filestore) must ensure licensing requirements are complied with fully.

2.3 Data Protection Act 1998

2.3.1 Registration

Users in possession of personal data must comply with the Data Protection Principles of the Data Protection Act 1998 and with any restrictions imposed to ensure adherence to the University's registration under the Act.

Members of staff are responsible for ensuring that holdings of personal data are registered internally with the Data Protection Officer who has the power to require modification or deletion of data in order to ensure compliance with the Act. The University's Data Protection Policy is available from the University's website at **www.reading.ac.uk/data_protection**

2.3.2 The Data Protection Principles

The Data Protection Act 1998 sets out eight Data Protection Principles. In summary these state that personal data shall:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
- be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes;
- be adequate, relevant and not excessive for those purposes;
- be accurate and kept up to date;
- not be kept for longer than is necessary for those purposes;
- be processed in accordance with the data subject's rights;
- be kept safe from unauthorised access, accidental loss or destruction;
- not be transferred to a country outside the European Economic Area, unless that country has adequate levels of protection for personal data.

2.4 Criminal Justice Act 1994

This Act amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to cover electronic communications as well as those on paper, and outlaws transmission and storage of pornographic or offensive material.

2.5 Regulation of Investigatory Powers Act 2001 and Lawful Business Practice Regulations 2002

The University's electronic communications systems (including the voice and data networks, email, web servers and internet connections) automatically and routinely log their usage. The University reserves the right to intercept, monitor and record electronic communications for lawful purposes as specified in the Act and Regulations and subsequent amendments.

2.6 Legal Responsibility

The University accepts no responsibility for the malfunctioning of any computing facility or part thereof, whether hardware, software or other nor for any consequential losses.

IT Services will follow recognised codes of practice concerning the archiving of magnetic disk files and the security of magnetic disks, tapes and other media, but cannot take responsibility for the security of an individual's data. Users are responsible for independently maintaining copies of valuable data.

IT Services does not operate a high security system and cannot give any warranty or undertaking about the security or confidentiality of data or other material it processes or that is deposited with it.

Where necessary IT Services reserves the right to compress, archive to tape or other media, or otherwise remove data stored on central filestore by existing or past users. IT Services also reserves the right to access, and where necessary to examine the content, of files or data held on central filestore, or on private devices connected to the campus network.

3. Contractual Responsibilities

3.1 Joint Academic NETWORK(JANET) Acceptable Use Policy (JAUP)

All members of the University are deemed to have agreed to the JAUP. (Appendix A).

3.2 Combined Higher Education Software Team (CHEST) Code of Conduct

All members of the University are deemed to have agreed to the Code of Conduct for the use of Software or Datasets issued by CHEST. (Appendix B).

3.3 User Regulations for the UK e-Science Grid

Any successful grid registration requires acceptance of the grid user regulations alongside the acceptable use policy of their own organisation. (See www.grid-support.ac.uk for up-to-date information).

3.4 Use of other institutions' facilities

Users may only use any other computing IT facility as permitted by the designated authority.

4. Authorisation to use IT Services facilities

4.1 Registration

4.1.1 Scope

No person or persons shall use IT Services facilities without authorisation.

All members and employees of the University shall normally be entitled to such authorisation in pursuance of their customary University work. Others may be permitted authorisation according to circumstances, and this may involve charges for use of facilities.

4.1.2 Means of Registration

Most students and some categories of staff will be registered on accepting a place or post at the University, and usernames and passwords will be issued upon arrival. Where a member of the University does not receive a username and password, they should apply for registration via IT Services Helpdesk in the Library.

Other applications should be made to the Director of IT Services in the first instance.

4.1.3 De-registration

IT Services reserves the right to remove user accounts on receipt of instructions from the School, Student, Academic Services or Human Resources, indicating that the user is no longer a member of the University. All data stored on centrally funded computing facilities is deemed to be the property of the University. IT Services will respond to formal requests from the Head of School or Service for retrieval of data stored by past or current members of that School or Service.

Members and employees of the University should be aware that their user accounts may need to be accessed by authorised staff following de-registration or in the event of any absence if such access is in the legitimate interests of the University.

4.1.4 Users' Responsibilities

Authorised users shall not allow use of their own usernames and passwords by any other persons and they shall not make use of others' usernames and passwords.

The facilities are provided for bona fide University purposes; educational, research and administrative uses. For any other use, special rules will apply and clearance must be obtained from the Director of IT Services [acting on behalf of the Information Strategy and Policy Committee (ISPC)] before any commitments are made to external sponsors. These special rules will cover payments due to the University for the use of its equipment and will protect the University from any claims for damages etc. which may arise from such use.

Any commercial exploitation of programs developed using University computing facilities is covered by the University's rules for the Commercial Exploitation of Intellectual Property.

Registered users are required to inform IT Services upon any change of status (for example from postgraduate to staff membership, or on departure from the

University). It is the responsibility of the user (or their School or Service) to instruct IT Services when an account or data is required to be maintained following that user's departure.

4.2 Charging

Users of chargeable computing resources (used for example for consultancy or other non-University work) or chargeable services (for example software, installation or printed output) shall pay IT Services upon demand at the rates agreed by the Advisory Group for IT Services.

5. Behaviour

All users of computing facilities are subject to the University Regulations for Conduct, including Sanctions, as listed in the University Calendar. With regard to computing facilities specifically, the following are examples of the consideration users are expected to show:

5.1 Use of resources

Resources are scarce and your usage may be at the expense of another. Resource allocation is made on the understanding that it is only to be used for academic purposes or special purposes for which it was requested.

Users need to be responsible about their use of:

- public machines; interactive computer use
- disk storage; processing time
- printers, printing materials and scanners; network bandwidth
- computer staff time; manuals and support materials

Irresponsible use wastes these resources and includes collection, creation, display and circulation of offensive material in any form or on any University equipment. It also includes playing games and abuses of news and electronic mail facilities, such as the sending of chain, junk or bulk e-mail.

5.2 Damage and Fault Reports

University computing facilities are provided for the community and all users need to take reasonable steps to avoid damage or prolonged outage. Installation (or modification of the set-up) of software, or connection of hardware to the campus network (directly or via another device) may only be made with the approval of the Director of IT Services.

Users should leave computers in a clean, usable state and report faulty equipment to IT Services. Users must not smoke, eat or drink in computing rooms, labs or areas.

5.3 Health and Safety

Computer users must obey health and safety regulations and procedures, as listed in the University Safety Guides available on the Health and Safety Services website and those posted locally or explained by IT Services staff.

All display screen equipment (DSE) users must ensure that a suitable and sufficient assessment of their work station has been completed. The workstation

must be set up in accordance with the Health and Safety (DSE) Regulations 1992 as amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002. Risks associated with poor workstation layout or working practices, such as musculoskeletal injuries, eye strain, fatigue and stress, must be reduced through workstation assessment and user training.

Do not disconnect machines, or attempt to repair damage or faults to any machine.

Children and animals are not permitted in any computer area except with the prior permission of the Director.

In short, never act in a manner which could jeopardise your safety or that of others.

5.4 General Consideration

Users should be considerate of others' legitimate use of computing facilities and the rights of all users to work undisturbed must be respected.

When you leave a machine you have been using (even for a short time), log off properly and ensure it is usable by others. This will protect your work as well as enabling fair use of equipment.

Opening and closing times of IT Services facilities (and associated security arrangements) must be respected.

6. Networked Information Provision

6.1 Information published on a University Information Server must be provided only by information providers recognised and approved according to the University's Web Information Policy (www.reading.ac.uk/webpolicy). Information providers will normally be representatives of Schools, Services, Centres or other groups within the University.

6.2 The University also has a policy regarding e.Information, available from the above website.

6.3 Complaints about content of networked information which does not conform to these policies should be directed in the first instance to webmaster@reading.ac.uk who will examine the pages involved and, if a breach appears to have taken place, will inform the provider and suspend access from the Information Service Menu Pages. In extreme cases or where a personal home page is involved the webmaster will request that IT Services suspend access to the page(s) from both the Information Provider and the wider public. In all cases the matter will be referred to the University's Web Information Steering Group (UWISG) and in extreme cases to the Information Strategy and Policy Committee (ISPC). Additionally action may be taken under paragraph 1.2 of these Rules.

Appendix A

JANET Acceptable Use Policy

Trademarks: 'JANET' and 'JANET(UK)' are trademarks of the Higher Education Funding Councils for England, Scotland and Wales, which have granted the JNT Association the right to use the marks.

Disclaimer: Neither the Higher Education Funding Council for England nor the JNT Association can accept any liability for any loss or damage resulting from the use of the material contained herein. The information is believed to be correct but no liability can be accepted for any inaccuracies.

Availability: Further copies of this document may be obtained from the JANET Service Desk, JANET(UK), Lumen House, Library Avenue, Harwell Science and Innovation Campus, Didcot, Oxfordshire, OX11 0SG.

Copyright © The Higher Education Funding Council for England, 1995–2007

Background and Definitions

1. 'JANET' is the name given both to an electronic communications network and a collection of electronic communications networking services and facilities that support the requirements of the UK higher and further education and research community. JANET is managed by JANET (UK) on behalf of the Joint Information Systems Committee (JISC) and is not for public use.

2. The Higher Education Funding Council for England, the Scottish Funding Council, the Higher Education Funding Council for Wales, the Department for Education, Culture and the Welsh Language and the Department of Employment and Learning Northern Ireland HE and FE branches are responsible jointly for the provision of JANET. They exercise this responsibility through their Joint Information Systems Committee (the JISC) and any dispute over the interpretation of this Policy will be resolved by the JISC.

3. JANET(UK) is the trading name of the company contracted by the JISC, acting in the name of the Higher Education Funding Council for England, for the provision of the JANET service. This includes the day-to-day management of this Policy.

4. This Policy applies in the first instance to any organisation authorised to use JANET (a 'User Organisation'). It is the responsibility of User Organisations to ensure that members of their own user communities use JANET services in an acceptable manner and in accordance with current legislation.

5. It is therefore recommended that each User Organisation establishes its own statement of acceptable use within the context of the services provided to its users, and in a form that is compatible with the conditions expressed in this Policy. Such a statement may refer to, or include, this document. If material from this document is included, this must be done in such a way as to ensure that there is no misrepresentation of the intent of this Policy. JANET(UK) can advise on this aspect as and where necessary.

6. JANET is maintained to support teaching, learning and research. The connection of any organisation to JANET is governed by the JANET Connection Policy maintained by the JISC. JANET is not a public network.

Acceptable Use

7. A User Organisation may use JANET for the purpose of interworking with other User Organisations, and with organisations attached to networks which are reachable via interworking agreements operated by JANET(UK). All use of JANET is

subject to payment of the appropriate charges in force during the period of service. Any provision of service must be authorised in advance.

8. 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.

Unacceptable Use

9. JANET may not be used for any of the following:

9.1. 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;

9.2. the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

9.3. the creation or transmission of defamatory material;

9.4. the transmission of material such that this infringes the copyright of another person;

9.5. the transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the User Organisation has chosen to subscribe;

9.6. deliberate unauthorised access to facilities or services accessible via JANET;

9.7. 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

JANET(UK) 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'.

10. 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. Any breach of industry good practice (as represented by the *standards of the London Internet Exchange*), or of the Acceptable Use Policies of other networks, that is likely to damage the reputation of the JANET network may be regarded as a breach of this AUP.

Passing on and Resale of JANET Service

11. It is not permitted to provide access to JANET for third parties without the prior agreement of JANET(UK), with the exceptions in the following sub-paragraphs.

11.1. The JISC has resale schemes whereby certain types of User Organisation may sell on JANET services under defined circumstances. Details may be obtained from JANET(UK).

11.2. It is acceptable for a User Organisation connected to JANET to extend access to others on a limited basis, provided no charge is made for such access. For example, it is acceptable that a visitor to the Organisation be permitted to gain access to JANET for the purpose of maintaining contact with his or her home organisation. It is intended that such use be regulated by the User Organisation in the same manner as it would regulate occasional use by third parties of its other facilities, such as its telephone and IT support systems.

12. A third party, where an individual, means someone who is not acting as a member of the User Organisation. Where it applies to a separate organisation, this is defined to be any organisation that is in law a separate entity to the User Organisation.

Compliance

13. It is the responsibility of the User Organisation to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of JANET does not occur. The discharge of this responsibility must include informing those at the Organisation with access to JANET of their obligations in this respect.

14. Where necessary, service may be withdrawn from the User Organisation. This may take one of two forms.

14.1. An indefinite withdrawal of service, should a violation of these conditions persist after appropriate warnings have been given by JANET(UK). Such a withdrawal of service would only be made on the authority of the JISC. Restoration would be made only when the JISC was satisfied that the appropriate steps had been taken at the Organisation involved to ensure acceptable behaviour in future.

14.2. A suspension of service, should a violation of these conditions cause serious degradation of the service to other users of JANET. Such a suspension would be made on the judgement of JANET(UK), and service would be restored when the cause of the degradation of service to others had been removed.

15. Where violation of these conditions is illegal or unlawful, or results in loss or damage to JANET(UK) or JANET resources or the resources of third parties accessible via JANET, the matter may be referred for legal action.

16. 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 B

Code of conduct for the use of software or datasets

The following text is a transcription of the CHEST Code of Conduct for the Use of Computer Software or Datasets. The Code was originally created with reference to

the use of software in Higher Education and Research Council Establishments, but is also applicable when Further Education institutions partake in CHEST Education Offers. The Code has been incorporated into the licence of all centrally-funded Eduserv Chest agreements. Many Higher Education establishments have in fact already amalgamated the Code into their regulations.

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

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 of 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 Eduserve 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 significant 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 or Courseware or other similar material, hereafter referred to as 'the Product', issued or otherwise made available to me by a School or Department of an Institution is subject to the following conditions:

1. I will ensure that all the requirements of the agreements or contracts and licences 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.)
2. I will adhere to the regulations governing the use of any service involved in the provision of access to the product whether these services are controlled by my own institution or by some other organisation.
3. I will not remove or alter the Copyright Statement on any copies of Product used by me.
4. 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, unless permitted to do so under the relevant licence.
5. I will use Product only for purposes defined, and only on computer systems covered, by the agreement, contract or licence.
6. I will only incorporate the Product, or part thereof, in any work, program or article produced by me, where this is permitted by the licence or by 'Fair Dealing'.
7. I will only incorporate some part or version of the Product in any work produced by me with the express permission of the Licensor or unless this is permitted under the Agreement.
8. I will not reverse engineer or decompile the software products or attempt to do so unless this is explicitly permitted within the terms of the Agreement for the use of the Product.
9. I will return or destroy all copies of the Product at the end of the course/year/ period of employment or when requested to do so.

Appendix C

Guidelines for the ongoing maintenance of School external facing websites

All external facing School websites have been produced by Communications and handed over for local maintenance by relevant Schools and Services.

One of the main goals of this project was to produce a standardised approach to University School and Service websites, bringing our end users a consistent experience to their journey through the University website. To this end, a standardised approach and information architecture framework was agreed with Heads of School was and implemented through the course of the School website rebranding project.

In order to ensure the standardised approach and consistency of experience is maintained, we ask that School and Service web information providers follow the guidelines below:

Please consult the Communications Office before you:

1. Alter your homepage
2. Alter the image on the homepage of each area (i.e. the entrance page for 'about us', 'undergraduate', 'postgraduate' etc)
3. Alter your navigation
4. Add or remove pages

You can contact Communications at webmaster@reading.ac.uk .

Please ensure that:

1. All content on your external website must be external facing information appropriate for your target audience
2. Content does not infringe copyright; all sources must be correctly acknowledged and any third party content must be cleared with the rights holder prior to use.
3. Where appropriate, that any documents available for download are branded
4. For accessibility purposes any documents uploaded should be available in PDF format. The link should display the filesize and format eg: 'Postgraduate prospectus (PDF-50KB)'.
5. Any images adhere to the guidelines available on the Branding website (www.reading.ac.uk/branding), especially for consent of use, resizing and compression of images
6. Please ensure any changes made locally are previewed before they are published

Further information:

- If you have any queries about these guidelines, please contact the Web Marketing Manager on webmanager@reading.ac.uk .
- If you have any about the ongoing maintenance of your website, please email ITS-Help.
- Training and drop in sessions for the Content Management System can be booked via the CSTD website: www.reading.ac.uk/cstd
- Further information about branding can be found on the Branding website: www.reading.ac.uk/branding

Appendix D

Web 2.0 Code of Conduct governing the use of Web 2.0 technologies by students at the University of Reading

What we will do for you:

- Provide Web 2.0 tools
- Promote the use of Web 2.0 amongst staff in order to better facilitate student learning and communication
- Communicate with you via email (the official channel), however, we will also use Web 2.0 technologies where appropriate to better spread these messages
- Provide the IT infrastructure so that you can access appropriate technologies

- Support the development of technical skills
- Handle complaints and investigate reports into inappropriate uses of Web 2.0 technologies

What we expect from you:

- Protect yourself-
 - Remember that not everyone is who they say they are. Before you join a group/accept a friend request check to see that they are who they say they are
 - Less is more. Don't put all your details online
 - Remember that your online presence may outlive your University career
 - Use third party applications sparingly (beware of viruses and phishing attempts)
 - Be aware of possible legal implications of your Web 2.0 activities
- Protect others-
 - Don't post other people's private details online (including 'tagging' of people in pictures)
 - Think before you post – be considerate of the feelings of others
- Get the most out of Web 2.0 tools by using them to-
 - keep in touch with friends, family, halls, tutors, clubs and societies
 - build your research/coursework (but check the reliability of sources)
 - build a strong online identity

Version	Keeper	Reviewed	Approved by	Approval date
1.0	ITS	Every four years	ISC	1/11/06
1.1	IMPS	Bi-annually	ISPC	16/11/11