

THE UNIVERSITY OF HULL

**Guidelines for the proper use of
computer facilities and services**

**4th edition
September 2009**

Changes to these Guidelines may be made from time to time, subject to the approval of the Director of Academic Services. Approved changes come into immediate effect and will be prominently displayed on the Customer Services website.

First edition:	September 1998
2 nd edition:	August 2000
3 rd edition:	September 2002
4 th edition:	September 2006, minor edits September 2009

Approved: by the Director of Academic Services, September 2006

INTRODUCTION

The use of University computer systems, networks and facilities is governed by the University Regulations which include these Guidelines. The Regulations and Guidelines apply to all staff and students of the University. By signing the declarations on the University registration form you have undertaken to abide by the Regulations and Guidelines. The Regulations and Guidelines also apply to affiliates of the University, including individuals associated with University committees, University libraries, alumni associations, student organizations, employee advisory groups, campus foundations and support groups.

The Guidelines extend the Regulations to provide information on what constitutes acceptable use of University computer systems, networks and facilities, guidance on policies such as monitoring and privacy, and the possible consequences of any misuse.

Failure to observe the University Regulations and Guidelines by a University employee, student, or other individual affiliated with the University may result in revocation of any computing account and/or disciplinary action. Such disciplinary action may include termination of employment or course of study, as appropriate and in accordance with University policies, regulations, or contracts. Any breaches of the criminal or civil law are beyond the remit of the University, but where criminal offences may have been committed, the University is legally bound to report some incidents to the authorities. If the Crown Prosecution Service decides upon a criminal prosecution this will be a matter for the department or individual concerned. Similar considerations apply to any civil law cases.

LIABILITY, WARRANTY AND RELATED MATTERS

Whilst every reasonable endeavour is made to ensure that the computing systems are available as scheduled and function correctly, no liability whatsoever can be accepted by the University for any loss or delay as a result of any system malfunction, howsoever caused.

Whilst every reasonable endeavour is made to ensure the integrity of software products, the University does not offer any warranty on any software or its support. Accordingly, no liability can be accepted in consequence of any such product producing incorrect results or failing to work as documented. The final responsibility for ensuring that any software is suitable for the purpose for which it is used, or that any result obtained on the computer system is correct, must always rest with the user.

Whilst every reasonable endeavour is made to ensure the integrity and security of information held on computer media, no consequent liability can be accepted by the University as a result of any such information being inadvertently lost, corrupted or inappropriately accessed.

Whilst every reasonable endeavour is made to ensure the accuracy of advice and information provided by the University, no liability can be accepted by the University for any consequential damages or losses arising from action or inaction by users based upon that advice and information.

The University reserves the right to dispose of spoilt work and waste media in any way of its choosing.

CONTENTS

INTRODUCTION	2
LIABILITY, WARRANTY AND RELATED MATTERS	2
CONTENTS	3
GENERAL GUIDELINES AND OVERVIEW	4
Overview	4
Authorised users.....	4
Personal use and payment for use	4
Software copyright.....	5
Unlawful or offensive materials.....	5
Computer Misuse Act 1990	7
Data protection.....	8
Privacy and Monitoring	8
SPECIFIC ACCEPTABLE USE GUIDELINES	10
Software use guidelines	10
Digital material use guidelines.....	11
General Internet use guidelines.....	16
Web publishing guidelines.....	17
Electronic messaging systems and data privacy guidelines.....	18
Guidelines for University Computer Systems Monitoring	21
REGULATIONS GOVERNING THE PROPER USE OF UNIVERSITY COMPUTER FACILITIES AND SERVICES	25
REGULATIONS GOVERNING THE CONNECTION OF DEVICES TO THE UNIVERSITY NETWORK	27

GENERAL GUIDELINES AND OVERVIEW

Overview

This document provides guidelines that must be followed to ensure that use of University facilities and services does not interfere with the activities of others and does not damage the reputation of the University. These guidelines include, where appropriate, interpretations of the current legal position. They are not an authoritative guide to that legal position, but are for general guidance.

As an employee, registered student or affiliate of the University you have the right to use certain of its computer systems, networks and facilities, but this right is conditional on your exercising it in a responsible way. If you misuse computing facilities or services you may commit a criminal offence and you may also contravene University Regulations.

Authorised users

As a member of staff or a registered student, you will normally be granted authorisation to use one or more of the University's computer facilities or services in pursuance of your employment or course within the University. An individual affiliated with the University may also be granted access to University facilities or services. In all cases you will have agreed to abide by the University's Regulations which includes these regulations and guidelines. Use of the University's facilities and services without authorisation will breach University Regulations and is also a criminal offence.

As an authorised user, you must also be aware of, and agree to abide by, the external rules applicable to users of University computer facilities and services. These will include, but may not be limited to:

- the UKERNA (JANET) Acceptable Use Policy
<http://www.ja.net/services/publications/policy/aup.html>
- the CHEST Code of Conduct for the use of Software or Datasets
<http://www.eduserv.org.uk/chest/conduct.html>

Personal use and payment for use

When you become an authorised user of university computing facilities, including computers and network services, you are only entitled to use them in pursuance of your course or employment in the University and for limited non-commercial personal use. Such personal use is only acceptable if it does not interfere with the operation of the University systems, and that the terms of the University Regulations and Guidelines are observed. Personal use by members of staff should not interfere with their job responsibilities.

The use of University computing facilities is, in general, free of charge, although some facilities (e.g. printing) may require payment of costs. If you wish to use a computer in connection with work for which you receive payment from an outside

body, you must inform the Head of your Faculty, and IT Systems (for the use of communal systems), before you undertake the work.

Software copyright

In general, systems and applications software (and many databases and datasets) are only licensed for use on the system upon which you find them. Unauthorised copying of such items with the intention to distribute them, even without charge, is a criminal offence under the Copyright, Designs and Patents Act 1988. If you are convicted of illegal copying, the penalties are severe. Unauthorised copying for private purposes is a civil offence and software companies are now much more rigorous in taking civil action.

Any original computer software will be protected by copyright. You must investigate whether you have the right to take a copy, and under what conditions, even in the case of software deemed to be 'Public Domain'. You should not assume that all Public Domain software is covered by identical terms in respect of copying and use. For further guidance see the 'Software use guidelines' below.

Unlawful or offensive materials

You commit a breach of University Regulations and may additionally be committing a criminal offence if you intentionally download, create, store or transmit certain materials on University computer facilities and services. Such materials will always include, but at the University's discretion may not be limited to:

- materials deemed offensive, obscene or indecent under The Obscene Publications Acts 1959 & 1964, The Sex Discrimination Act 1975, The Race Relations Act 1976, The Protection of Children Act 1978, The Public Order Act 1986, the Criminal Justice and Public Order Act 1994, the Sex Offences Act 2003 and any subsequent relevant legislation that may come into force throughout the duration of these Guidelines. You should be aware that the University is legally obliged to inform the police if indecent material (child pornography) that involves, or appears to involve, children (defined as 'people apparently under the age of 18') is found on University computer facilities. Making an indecent image of a child carries a maximum sentence of 10 years imprisonment. The term 'make' includes downloading images from the Internet and storing or printing them out.
- material deemed unlawful under The Contempt of Court Act 1981, The Data Protection Act 1998, The Telecommunications Act 1984, The Copyright, Designs and Patents Act 1988, The Computer Misuse Act 1990, The Trademarks Act 1994 and any subsequent relevant legislation that may come into force throughout the duration of these Guidelines.
- defamatory material, i.e. material that falsely states or implies something about an identifiable individual that will result in that individual being held in lower esteem by others as a result;
- material that is otherwise sexist, racist, homophobic, xenophobic, or similarly discriminatory;

- material that advocates or condones, directly or indirectly, criminal activity, or which may otherwise damage the University's research, teaching, and commercial activities, in the UK or abroad;
- materials to which a third party holds an intellectual property right, without clear evidence of permission, or a licence, from the rightholder. Thus copyrighted material, such as novels, poetry, non-fiction books, letters, memoranda, directories, e-mail messages, photographs, paintings, films, video, sound recordings, cartoons etc. should be used only where you are sure that copyright has expired, or that you have explicit permission to use them; and trademarked logos such as those used by Microsoft®, Coca Cola®, and Adobe® should not be used without permission;
- material primarily designed, produced, or adapted for the purpose of enabling or facilitating the circumvention of effective technological measures for the protection of copyrighted works. This includes, but is not limited to: software designed to remove copy protection from music files, such as Fairuse4wm;
- material that could be used in order to breach computer security, or to facilitate unauthorised entry into computer systems. This includes, but is not limited to: viruses; virus creation kits; User IDs and passwords obtained without authorisation, or which you have no authority to disclose to others; and "hacker manuals";
- material that is likely to prejudice or seriously impede the course of justice in UK criminal or civil proceedings. This includes: material which prejudices a case, especially where it makes the express or tacit assumption that the accused in a criminal trial is guilty; material which is emotive or disparaging, especially where there is an insinuation of complicity or guilt by association; material which is likely to be inadmissible at trial, such as previous convictions, or mention of evidence likely to be excluded as having been improperly obtained; material such as a photograph of the defendant, where the issue of identification forms part of the trial proceedings; material hostile or abusive towards potential witnesses with the intention of coercing them into not testifying, or disclosure of witnesses' names following a court order that their names should not be disclosed; material disclosing information about jury deliberations; material breaching reporting restrictions in cases where in open court there is identification of children involved in the proceedings, or identification of rape victims;
- personal data (as defined by the Data Protection Act 1998) relating to third parties, unless their explicit permission has been given, or the information is properly registered with the Information Commissioner, or the information is covered by a relevant exemption.

If you believe your legitimate work at the University requires access to material that may be deemed unlawful or offensive you should first seek advice from the Service Desk in the Brynmor Jones Library or the Helpdesk on the Scarborough campus.

Should you, in the course of your legitimate work, encounter material on a University computer that appears to be indecent, you should inform the Service Desk immediately. The law provides protection against prosecution for staff in systems management who have a role in identifying and securing such data for evidential and

investigative purposes, but that protection only applies to specific staff, and even then only if correct procedures are precisely followed. Personal investigations by unauthorised staff, however well intended, will expose them to criminal prosecution.

Computer Misuse Act 1990

The University and users of its resources are required to comply with the Computer Misuse Act 1990. The actions described below are likely to fall foul of the Act – if in doubt you should seek further advice.

Unauthorised access to computer material

Many computers in the University provide access to computer networks that enable you to connect to computers at other educational establishments, but also to connect computers at many sites not related to the education sector. The ability to connect to a computer does not automatically give you the authority to use it. If you access, or attempt to access, a computer that you are not authorised to access, you will breach University Regulations and also commit a criminal offence. If you are convicted of this offence in the criminal courts the legal penalties are severe.

Some computers offer freely available services, such as websites or library catalogues. Many systems will make it clear that they are public access. If a system is not obviously public access, or if it displays a message that explicitly states that you need to be authorised to use it, you should not attempt to use the system.

You commit an offence against University Regulations, and a criminal offence, if you deliberately use a computer to access any program or information that you are not authorised to use. You may access any information or program that you yourself have written, or which is freely available on the computers you are authorised to use. You must not access, or copy, information or programs belonging to other users without their permission, preferably in writing. If you are convicted of this offence in the criminal courts the legal penalties are severe.

You must not use another user's user-id and password, even if they make them available to you, unless expressly authorised by IT Systems to do so (for example, where you need to use a user-id and password allocated to another person in order to carry out a job function, such as website maintenance, during their absence from the University) In such circumstances, permission should normally have also been obtained, in advance, from the person whose user-id and password is to be used. If one user gives details of their password to another user who uses them to gain access to University facilities or services then both users are guilty of an offence against the University's Regulations. If for any reason you wish to use another user's information or programs, you must get the user's permission. You are reminded that attempting to discover another user's password, by any means, is an offence.

Unauthorised modification of computer material

You commit an offence against University Regulations and a serious criminal offence if you alter data, programs, files, electronic mail or any other computer material belonging to another user, without the other user's permission. This also applies to the system data and programs. If you are in any doubt as to whether or not you are allowed to alter another user's computer material do not do so. If you are convicted of this offence in the criminal courts the legal penalties are very severe. The wilful

introduction of computer viruses on to computer systems is covered by this section of UK computer misuse legislation - together with its penalties.

Unauthorised access with intent to commit or facilitate commission of further offences

You commit an offence against University Regulations, and a serious criminal offence, if you access computer material without authorisation as a preparation for some more serious offence, for example to commit a fraud. If you are convicted of such an offence the legal penalties are very severe.

You must not access a computer without authorisation as a preparation towards committing a criminal act. If you do the penalties are very severe, comparable to those for the criminal act for which you may be preparing. In such cases the matter would normally be passed to the police. The University may impose further penalties, up to and including exclusion or dismissal from the University, even in cases where there is no prosecution or conviction.

Data protection

The Data Protection Act 1998 provides a set of rules ('data protection principles') for the recording, storage, and processing of information that relates to identifiable individuals ('personal data'). Failure to observe the data protection principles may result in both criminal charges and civil actions for compensation. If you intend to undertake work on a University computer which involves the recording, storage, or processing of personal data, you should discuss your plans with the University's Data Protection Officer, or consult the Office of the Information Commissioners web site:

<http://www.dataprotection.gov.uk/>

You must not attempt to obtain access to any data relating to the administration of the University, unless it is available through public channels, or you have been explicitly told that you may do so. The University's Freedom of Information Publication Scheme identifies which University information is publically accessible:

<http://www.acsweb.hull.ac.uk/foia/publicationscheme/index.html>

You have the right under the Freedom of Information Act to request information, other than your personal data, concerning the University that is not publically accessible. Such requests should be made to the Records Manager, Brynmor Jones Library. The University will have notified the Information Commissioner's Office about its administrative processing of personal data under the Data Protection Act 1998, and you have the right under the Act to request a copy of the records relating to you that the University maintains. Such requests should be made to the University's Data Protection Officer.

Privacy and Monitoring

Users may not, under any circumstances, monitor, intercept or browse other users' data including e-mail messages. Network or system administrators may not normally monitor other users' data other than to the extent that this may inevitably occur in the usual course of their work. Monitoring, interception and reading of other users' data by network or system administrators is described later in the section titled *Guidelines for University Computer Systems Monitoring*.

The University of Hull hereby notifies all users of its telecommunications and computer facilities and services that it reserves the right to monitor all communications on those facilities, in accordance with its monitoring policy below. Authorised users of the system should be aware that personal communications, as well as communications related to the functioning of the University, made via the University's telecommunications and computer facilities, may be intercepted and/or monitored by IT Systems staff, or other technical staff, as lawfully authorised by the University.

The University has the right to access and disclose data within a user's account (including e-mail messages) as required by University legal and audit obligations, and for legitimate University operational purposes. This may include periods when a user may be absent from work, e.g. through illness, and particularly when someone leaves the University. This area is discussed in more detail later in the section *Electronic messaging systems and data privacy* guidelines

If you are in any doubt as to whether your intended actions are acceptable and/or legal then you should seek advice from the Service Desk before you proceed.

SPECIFIC ACCEPTABLE USE GUIDELINES

Software use guidelines

The making, use, and possession, of any copy of computer software without the licence of the owner of the program is illegal, and may leave both you and the University open to criminal and civil proceedings. It is therefore of the utmost importance that you comply with the following guidelines:

You may not make, or use, any more copies of any computer software than the relevant licence permits, and, except where otherwise allowed by legislation, you must comply with the terms and conditions held in that licence.

If you are in any doubt as to whether permission has been granted, either by the original licence, or by other written communication from the copyright holder, no copies should be made.

The Copyright, Designs and Patents Act 1988 s50A permits a lawful user of a program to make a copy of it for backup purposes, even where the license purports to forbid such action. Any term of an agreement that prohibits or restricts the making of a back up copy of a program is void (s296A CDPA). If you are in any doubt as to the meaning or scope of the licence, or any relevant legislation, you should not make copies.

Computer software may only be placed on University systems, or held on University premises, in circumstances where a valid licence is held. Unlicensed copies of computer software must not be brought on to University premises; uploaded to or downloaded from University systems; or passed across University networks. Computer software may only be used for University business, or for your work with the University, either on University premises or elsewhere, if you hold a valid licence.

If you are in any doubt as to whether computer software in your possession is held under a valid licence, it should not be used until you have verified that it is a legal copy. If it is not a legal copy, it should be destroyed.

You may not distribute, sell, hire out or otherwise deal with any unauthorised copy of computer software.

If you are in any doubt as to whether computer software in your possession is held under a valid licence, no dealings with that software should be undertaken, until you have verified that it is a legal copy. If it is not a legal copy, it should be destroyed.

Members of staff are not authorised or permitted to allow any student to engage in copyright infringing acts.

Breach of any of the above Guidelines may lead to University disciplinary proceedings being brought against you. If you are in any doubt as to whether your intended actions are acceptable and/or legal you should contact the Service Desk for advice.

Digital material use guidelines

The definition of digital materials for the purposes of these guidelines does not include computer software. Computer software has its own separate section above.

Copyright Legislation and Fair dealing

In the UK, Copyright regulations are governed by the Copyright Designs and Patents Act 1988 (CDPA) and its subsequent amendments. There are concessions for users under the CDPA known as 'fair dealing'. Fair dealing is a defence against a copyright infringement action. An individual can claim this defence so long as the copying does not damage the legitimate commercial interests of the rightsholder, and if it was for one of the specified purposes. The burden of proof is on the person who copied to show that it was for one of the specified purposes and that it did not damage the rightsholder. If they cannot show this, then they have infringed the rightsholder's copyright. The CDPA does not define fair dealing precisely, but the Act sets out both general fair dealing defences, and defences that are specifically available for educational purposes.

General fair dealing defences

The general fair dealing defences include that:

- Copying of a literary, dramatic, musical or artistic work for the purposes of research for a *non-commercial* purpose, or private study, does not infringe any copyright in a work;
- Copying of a work for the purpose of criticism or review of the work, or another work, or of a performance of a work, where the work has been made available to the public, and the copy is accompanied by a sufficient acknowledgement, does not infringe any copyright in a work;
- Copying of a work for the purpose of reporting current events (other than the use of a photograph) accompanied by a sufficient acknowledgement does not infringe any copyright in a work.

The fair dealing concessions apply equally in the digital environment as in the non-digital environment, so use of a third party work on a website, in the course of criticism or review of that work, or another work, could fall under the 'criticism or review' fair dealing defence. Obviously some common sense has to be employed - for the fair dealing defence the material should be necessary for the criticism or review and used proportionately, i.e. criticism of a poem might require quite extensive quotation, but criticism of a journal article is unlikely to require the inclusion of a large part, or the whole, of the article.

Please note that the fair dealing provisions do not cover the copying of electronic images and text (for example from the internet) for inclusion into a new resource (for example a Virtual Learning Environment). This would be regarded as re-publishing the information for a new audience. Further information is provided within the Brynmor Jones Library pages at www.hull.ac.uk/lib

You may not make, or use, any more copies of any digital material than permitted by fair dealing provisions or by relevant permissions and licences from the copyright holder. Where digital material is obtained under licence conditions you must comply with all the terms and conditions held in that licence, including restrictions on printing, downloading, cut-and-paste and networking.

You may not create digital materials on University equipment, or on University premises, by electronic copying or scanning hardcopy works unless this is permitted by fair dealing provisions or by relevant permissions and licences from the copyright holder.

If you are in any doubt as to whether you can copy or scan hardcopy works to create digital material you must check the Copyright section of the library homepage at <http://www.hull.ac.uk/lib>.

Digital material may only be placed on University equipment, or held on University premises, where permitted by fair dealing provisions or by relevant permissions and licences from the copyright holder. Infringing material must not be brought on to University premises; uploaded to or downloaded from University systems; or passed across University networks.

Digital material may only be used for University purposes, or for your work with the University, either on University premises or elsewhere where permitted by fair dealing provisions or by relevant permissions and licences from the copyright holder

If you are in any doubt as to whether you can hold, or make copies of, digital material you must check the Copyright section of the library homepage at <http://www.hull.ac.uk/lib>. If existing digital materials are identified as infringing copies they must be deleted or destroyed.

You may not distribute, sell, hire out or otherwise deal with any infringing copy of digital material.

Digital material held under fair dealing provisions may not be further copied, distributed, sold or hired, to do so is a breach of copyright. Digital material obtained under licence, or with permission, may only be further copied, distributed, sold or hired if the licence or permission permits this.

Members of staff may not make, or provide, multiple copies of digital material for the purposes of student study, research or criticism except under a valid licence, or with the written permission of the copyright owner, or where permitted by fair dealing provisions.

Provision of digital material that involves the making of more than one copy for a single individual will not be fair dealing. Thus making a copy for each member of your class, even if spread over time, will be an infringement.

Members of staff are not authorised or permitted to allow any student to use any digital material on University premises or University equipment, which is not permitted by fair dealing provisions or for which appropriate permissions or licences from the copyright holder have not been obtained by either the student, yourself, or the University.

Members of staff are not authorised or permitted to allow any student to copy any digital material on University premises or via University equipment, which is not

permitted by fair dealing provisions or for which appropriate permissions or licences from the copyright holder have not been obtained by either the student, yourself, or the University.

No member of University staff may give, or purport to give, permission for students to engage in copyright infringement.

Examples of acceptable and unacceptable digital material creation and use

If you have the written permission of, or a licence from, the copyright holder to make single or multiple electronic copies or scans of all, or part of, a hardcopy work, you must adhere strictly to the terms of the permission or licence regarding their use and distribution. If you do not have the written permission of, or a licence from, the copyright holder you may make an electronic copy or scan part of a hardcopy work only if that electronic copying or scanning is for the purpose of your research or private study, and the resulting digital copy is used only by yourself.

- *Electronic copying or scanning all of a hardcopy work e.g. all of a book, or all the articles in a journal issue, is not fair dealing;*
- *Electronic copying or scanning of part of a hardcopy work for use by multiple users is not fair dealing;*
- *Electronic copying or scanning of part of a hardcopy work with the intention that it be placed on a network or on the Web is not fair dealing;*
- *Making and distributing further digital or hardcopy copies of electronically copied or scanned material is not fair dealing.*

If the only copying carried out, whilst viewing part or all of an electronic publication, is the incidental copying of the material to computer memory or to hard disk by the program (e.g. a Web browser or proprietary viewer) for operational purposes, and those copies are of a transient nature, this will be fair dealing.

- *If you access an electronic journal available on a Web site using a University PC and the browser automatically copies the article to your hard disk when you view the article. - this is fair dealing;*
- *If you view all of the articles of an electronic journal available on the Web using your browser and it automatically copies all the articles to your hard disk cache as you view them - this is fair dealing;*
- *If you log into the university/library network and access an electronic journal and the browser or viewer automatically copies all the articles you view to a network cache - this is fair dealing.*

If you print on to paper one copy of part of an electronic publication, for your research or private study, this will be fair dealing

- *If you access an electronic journal available at a Web site using a University PC and print out a hard copy of an article for research or private study - this is fair dealing;*

- *If you log into the library/university network, access an electronic journal available at a Web site, and print out a hard copy of an article for research or private study - this is fair dealing;*
- *If you access an electronic resource to which the University of Hull has a paid subscription you can print out hard copy of some of the material from the resource for research or private study, assuming this is allowed by the licence agreement. If you are uncertain about whether you may print, or the amount you may print, you should obtain advice from the Brynmor Jones Library;*
- *A friend may print you a hard copy of digital material for your research or private study - this is fair dealing. However, if your friend knows, or has reason to believe, that you intend to then make multiple copies of that copy for distribution, then this is not fair dealing (s29(3)(b) CDPA 1988).*

If you copy part of an electronic publication onto permanent local electronic storage accessible to only one user at a time – this will be fair dealing

- *If you access an electronic journal available at a Web site using a University PC, you can save a copy of an article to your personal network space or to a memory stick for research or private study- this is fair dealing;*
- *If you visit the Brynmor Jones Library and access an electronic resource to which the University of Hull has a paid subscription you can save a copy of some of the material to floppy disk and take it away with you for research or private study, assuming this is allowed by the licence agreement. If you are uncertain about whether you may save to disk or the amount you may save to disk you should obtain advice from the Library;*
- *A friend may save a copy of digital material to disk for your research or private study - this is fair dealing. However, if your friend knows, or has reason to believe, that you intend to then make multiple copies of that copy for distribution, then this is not fair dealing.*

It is not fair dealing for an individual to copy on to disk all of an electronic publication for permanent local electronic storage.

- *If you want to download an entire Web site, you must contact the owner of the Web site for permission;*
- *If you view an entire Web site and your Web browser automatically copies all the pages to your hard disk cache as you view them – this is fair dealing, unless you do so with the intent of using the transient files to create an infringing copy;*
- *If you want to download an entire electronic journal, you must contact the owner of the electronic journal for permission;*
- *If you want to download an issue of an electronic journal, you must contact the owner of the electronic journal for permission - it is unclear whether this is fair dealing.*

You may not place part or all of an electronic publication in which you do not hold the copyright, or for which you have not obtained permission from the rightsholder, on a network or Web site open to the public.

- *If you want to put some of your work on the Web or an intranet you may do so if you retain the copyright in that work. If you have assigned your rights, or granted an exclusive licence in that work, you can only do so if you have specifically retained this right, or if you contact the new copyright owner and ask permission;*
- *You may not put other people's work on the Web or an intranet without getting the permission of the copyright owners first;*
- *You may not cut-and-paste portions of other Web sites into your own, unless explicitly permitted to in the copyright notice on those sites or without getting the permission of the copyright owners first.*

Breach of any of the above Guidelines may lead to University disciplinary proceedings being brought against you. If you are in any doubt as to whether your intended actions are acceptable and/or legal you should contact the Service Desk for advice.

General Internet use guidelines

The University of Hull seeks to provide all staff and students with appropriate access to the Internet for the purpose of facilitating their work and studies. Although Internet usage and e-mail messages are not routinely monitored, the University reserves the right to intercept any internal communications for inspection in the event that abuse of the facilities or services is suspected. Users are directed, in particular, to the information contained in the section *Guidelines for University Computer Systems Monitoring*.

Staff and students may not use University access to the Internet:

- to access, retrieve, store, print and material that may be deemed offensive and/or unlawful as described in the section 'Unlawful or offensive material'
- for personal gain or for business activities unrelated to University operations;
- to post information or participate in debate in any way that could be construed as acting on behalf of the University except for staff given the express permission of their Dean of Faculty or Head of administrative section, or of the Registrar, to do so;
- to download, or distribute unlicensed or pirated software and files (e.g. unlicensed audio materials such as .mp3 files);

The University reserves the right to block access to any Internet resource. Access to blocked sites will be considered by application to the Director of Academic Services.

Breach of any of the above Guidelines may lead to University disciplinary proceedings being brought against you. If you are in any doubt as to whether your intended actions are acceptable and/or legal you should contact the Service Desk for advice.

Web publishing guidelines

You may only publish web pages on University computing equipment that has been specifically designated for that purpose. You are not permitted to designate, represent or hold out any personal web pages as being official University web pages. Personal web pages may not be used for official University business, or to enter into contracts, which purport to bind the University.

Web pages hosted on designated University computing equipment may not:

- contain, or be used to distribute, or have direct links to, material that may be deemed offensive and/or unlawful as described in the section 'Unlawful or offensive material';
- be used for placing and distribution of commercial advertisements or to otherwise promote commercial companies or materials;
- use University logos, or other copyrighted or trademarked University materials without permission.

You should ensure that web pages, as is the case for course materials and other information, are accessible and do not discriminate against students because of disability.

If you believe that a member of the University has personal web pages hosted on University computing equipment which contravene these conditions, you should report your concern, indicating the location and nature of the offending material, to the Service Desk who will ensure that it is promptly dealt with by the relevant individual responsible for the area at issue, and that any necessary disciplinary action is taken.

Breach of any of the above Guidelines may lead to University disciplinary proceedings being brought against you. If you are in any doubt as to whether your intended actions are acceptable and/or legal you should contact the Service Desk for advice.

Electronic messaging systems and data privacy guidelines

Introduction

The term 'electronic messaging systems' is used within this section to apply to any system used for personal communication over the Internet. This includes, but is not limited to, electronic mail (e-mail) and instant messaging systems, but excludes, for the purposes of this document, telecommunications e.g. telephone and SMS/text services. This section sets out the University's guidelines on the proper use of such systems for University purposes.

The intent of this section is to assure that:

- the use of such systems is related to University purposes;
- University resources are used effectively and disruptions to University activities are avoided;
- the University community is informed about confidentiality, privacy, and acceptable use of these systems.

Overview

There are a number of characteristics that distinguish electronic messaging systems from other means of communication, such as paper records and telephones. Awareness of these traits should guide an individual's use of e-mail.

To prevent loss of data, as part of standard computing and telecommunications practices, systems involved in the transmission and storage of messages are "backed up" on a routine basis. The back-up process results in the copying of data, such as the content of an e-mail message, on to storage media that may be retained for periods of time and in locations unknown to the originator or recipient of a message. The frequency and retention of back-up copies vary from system to system. While it may be difficult and time consuming, it should be assumed that back-up copies of a message that exist could be retrieved even though the recipient has discarded his/her copy of that message.

It is usual practice for individual accounts to be password protected. While this security measure is beyond the usual measures taken to protect access to paper records and telephones, it does not confer a special status on messages stored within that account with respect to the applicability of laws, policies, and practices.

In the usual course of their work, network or system administrators may monitor the performance of a network or messaging service. It can be assumed, therefore, that the content of messages may be seen by such individuals during the performance of these duties.

Electronic messaging systems, including e-mail should not be considered inherently secure. For example, it is possible for unauthorised individuals to monitor the transmission of e-mail or to send counterfeit e-mail under someone else's e-mail address. Therefore, users should not include any confidential or personal information in an electronic message. Use an alternative method of communication to send confidential information.

Appropriate use of electronic messaging systems

Electronic messaging systems are subject to all the same laws, policies, and practices that apply to the use of other means of communications, such as telephones and paper records. Expressions of fact, intention and opinion within a message may have legally binding effects for you and/or the University, and could be produced as evidence in court. Users must therefore ensure that their use of such systems is consistent with appropriate use of University resources and facilities.

For example, users may not use University resources and facilities, to transmit:

- material that may be deemed offensive and/or unlawful, as described in the section 'Unlawful or offensive material'
- information, or to participate in debate, in any way that could be construed as acting on behalf of the University except for staff given the express permission of their Dean of Faculty or Head of administrative section, or of the Registrar, to do so;
- commercial material unrelated to the legitimate business of the University;
- bulk messages unrelated to the legitimate business of the University which is likely to cause offence or inconvenience to those receiving it e.g. spamming;
- unsolicited e-mail messages requesting other users, at the University or elsewhere, to continue forwarding such e-mail messages to others, where those e-mail messages have no educational or informational purpose (chain e-mails);
- messages which purport to come from a individual other than the user actually sending the message, or with forged addresses (spoofing);

Electronic messaging systems and privacy

The University provides access to electronic messaging systems for the conduct of University business. Incidental and occasional personal use of such systems, particularly e-mail, is permitted within the University so long as such use does not disrupt or distract the conduct of University business (i.e., due to volume or frequency). However it is important to understand that such personal use will still be subject to the monitoring policy described in *Guidelines for University Computer Systems Monitoring*. In addition, the University has the right to access and disclose the contents of a user's e-mail messages as required by University legal and audit obligations, and for legitimate University operational purposes.

Access to stored documents (including e-mail) for business purposes

There are occasions when the University needs to access information held by a member of University within electronic mail, elsewhere on his/her computer, or in other filestore or backup media. This will usually occur when an employee is absent, either ill or on leave, and a situation arises which requires a rapid response. Members of the University must be made aware that the University reserves the right to obtain access to files held on/in equipment owned by the University, and that the privacy of

personal material stored on/in such equipment in the event of authorised access cannot be guaranteed.

Persons facilitating such access, usually IT Systems staff, will require written authorization on each occasion. It may be possible to obtain authorization from the absent individual, but will more normally be sought at the level of the Head of Faculty or Service. The latter authorization must identify the material to be accessed, its location and why a delay in access would be detrimental to the University's interests. It is intended that these arrangements are for exceptional circumstances only: normal business processes should avoid their necessity through use of role-based shared e-mail addresses or lists, appropriate file access control, etc.

Persons facilitating access must take all reasonable measures to respect privacy. However, difficulties may arise when searching for material, as there is no guaranteed method of distinguishing between business and personal items. Users are advised to minimise the risk of inadvertent viewing of private material by placing appropriate messages or files in folders (or directories) whose name includes "Personal". (Mail filters can be set up to move messages automatically into folders according to sender or destination address, etc.)

Electronic Mail Addresses

The University of Hull owns its users' University e-mail addresses. When a user's affiliation with the University is terminated, to the extent technically and financially feasible, the University may accommodate the redirection of e-mail to a new e-mail address identified by that user for a reasonable period of time as determined by the Director of Academic Services.

A student's e-mail address is considered a student record and is thus subject to University policies and procedures in regarding the disclosure of information from student records.

Breach of any of the above Guidelines may lead to University disciplinary proceedings being brought against you. If you are in any doubt as to whether your intended actions are acceptable and/or legal you should contact the Service Desk for advice.

Guidelines for University Computer Systems Monitoring

Introduction

In the business environment, companies routinely monitor data held on their equipment and inspect e-mail and other electronic data entering, leaving, or within, their networks. This activity in public and private organisations is regulated by the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

The Regulation of Investigatory Powers Act 2000 does, however, allow for legitimate interceptions of communications by organisations on their private telecommunications networks – in other words, it provides ‘lawful authority’. A general exception is made in the Act for interception where the interception is by or on behalf of a person running a telecommunications service for purposes connected with the provision or operation of that service:

- e.g. e-mail postmasters may examine mis-addressed messages in order to redirect them as necessary, or check e-mail subject lines for malicious code;
- e.g. system operators may monitor system traffic to determine its source, where this is necessary to ensure the effective performance of their mail servers, for example to eliminate unsolicited commercial e-mail (‘spam’).

Further, if the controller of the telecommunications or computer system has made reasonable efforts to inform potential users that interceptions may be made, and thus they have no reasonable expectation of privacy in relation to their communications, the following actions are permitted:

Institutions may monitor and record communications:

- to establish the existence of facts to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved;
- in the interests of national security;
- to prevent or detect crime;
- to investigate or detect unauthorised use of telecommunication systems;
- to secure, or as an inherent part of, effective system operation.

Institutions may monitor but not record:

- received communications to determine whether they are business or personal communications;
- communications made to anonymous telephone helplines.

The University of Hull hereby notifies all users of its telecommunications and computer facilities and services that it reserves the right to monitor all communications on those facilities, in accordance with its monitoring policy below. As such authorised users of the system should be aware that personal communications, as well as communications related to the functioning of the University, made via the University's telecommunications and computer facilities, may be intercepted and/or monitored by IT Systems staff, or other technical staff, as lawfully authorised by the University.

The University of Hull thus has the legal right, at any time, to inspect all data held on University computer equipment, and to inspect all e-mail and other electronic data entering, leaving, or within, the University network to ensure conformity with:

- University regulations;
- Contractual agreements with third parties;
- UK law.

The University is obliged by virtue of the agreement entered into with UKERNA to ensure as far as possible that its users do not use the SuperJANET system to transmit or transfer certain types of electronic data.

The University is obliged by law to report to the police the discovery of certain types of electronic data, if that data is found on University equipment, or transmitted across University networks.

Many types of routine computer service tasks will involve IT Systems staff members and other members of University technical staff having access to various levels of staff and student held data.

Examples include:

- e-mail postmasters receiving mail failure notifications will often be sent text of the failed message by the e-mail server which has rejected or redirected it;
- staff making archive copies from file servers will, as part of the archiving process, often be able to read the names of files held in staff and student accounts;

This document contains the University's Computer Systems Monitoring policy. The policy is designed to describe to staff and students:

- the monitoring measures that the University has decided are acceptable;
- the types of circumstances as a result of which monitoring may be instituted;
- the procedures that ensure that monitoring is carried out only under those circumstances, and prevent abuse of the monitoring process.

The policy

It is University policy that IT Systems staff, and relevant staff in other administrative and academic units, may not routinely access staff and student data held on University computer equipment, or routinely inspect the contents of e-mail and other electronic data entering, leaving, or within, the University network. Attempts by any member of

staff to implement any such system of monitoring will be in breach of this policy and may be the subject of disciplinary proceedings.

The University recognises that, due to the nature of computer systems, data held on its computer systems, passing across its networks, or printed out on University equipment, may at times be visible in readable form. In such circumstances, that data may well be viewed by IT Systems staff or by relevant staff in other administrative and academic units. Such incidental viewing will not constitute a breach of this policy, even where such viewing leads to the implementation of authorised monitoring (as described below) and/or disciplinary procedures against the user concerned.

The University reserves the right to monitor and access data held on its computer equipment, and data entering, leaving, or within, the University network in the following circumstances:

- Where, by virtue of carrying out routine computer service tasks, members of IT Systems and other members of University technical staff discover data which breaches University regulations, the University's contractual obligation to third parties, or UK law, or where the nature of the data suggests such a breach has occurred or will occur;
- Where complaints are received by the University authorities suggesting that the University's computer systems or networks are being used to store, transmit or transfer data which breaches University regulations, the University's contractual obligation to third parties, or UK law;
- Where the University has been requested, or required, to monitor data by the police as part of a criminal investigation;
- Where there is other reasonable suspicion that users are storing, transmitting or transferring data which breaches University regulations, the University's contractual obligation to third parties, or UK law.

The University reserves the right to monitor the nature and extent of data uploaded and downloaded from the Internet. This may be carried out by various means, including random filename searches of file servers and file size checks.

Oversight

Specific monitoring of user data, and specific access to user data, by IT Systems staff may only be legitimately carried out under this policy with the knowledge and written consent of at least one of the following:

- the Registrar of the University;
- the Director of Academic Services;
- the Director of IT Systems.

Specific monitoring of user data, and specific access to user data, by staff of other administrative or academic units may only be legitimately carried out under this policy with the knowledge and written consent of at least one of the following:

- the Registrar of the University;
- the Director of Academic Services;

- the Director of IT Systems;
- the head of the academic or administrative unit which owns the computing equipment on which the data is stored, or from which it is transmitted, or transferred.

Specific monitoring of, or specific access to, user data should only take place for such time as is required to ascertain whether the user or users concerned are storing, transmitting or transferring data which breaches University Regulations, or the University's contractual obligation to third parties, or UK law. Long term monitoring should only be permitted when this is specifically requested by the police as part of an on-going criminal investigation.

Where, by virtue of carrying out routine computer service tasks or in the course of undertaking approved monitoring, members of Academic Services and other members of University staff (such as Faculty or Departmental network administrators) suspect or have reason to believe that security or integrity of the University network systems has been breached then one or more of the following actions may be taken.

- Accounts of users may be suspended without prior warning until the event has been fully investigated;
- Devices connected to the University network may be physically disconnected without warning;
- Devices belonging to University of Hull may be impounded for investigation without warning and kept to be used as evidence until such time as any incident has been fully resolved;
- Devices may be required to be wiped clean of data, programs and settings before being allowed to connect to the University network;
- Any third party may be involved at the discretion of the University, for example CERT-UK or the police.

All of the above actions can occur whether the user has been knowingly or unknowingly involved in the events leading up to the security breach. Any of the actions can also be taken in relation to University of Hull devices with or without the consent of the current user of that device.

In the case of a security breach, for example a denial of service attack, the first and foremost priority is the protection of the University network and systems. IT Systems staff may need to act quickly and be unable to give prior warning of any actions. It is expected that all members of the University community will co-operate fully in the case of such an event occurring.

REGULATIONS GOVERNING THE PROPER USE OF UNIVERSITY COMPUTER FACILITIES AND SERVICES

1. All staff and registered students will normally be granted authorisation to use shared computer facilities and services provided by the University, unless specifically excluded from doing so. All other persons must seek permission from the Director of Academic Services before using any facilities. Authorisation for any person to use University computer facilities and services is, however, conditional upon adherence to these Regulations, and all users shall be presumed to know these Regulations.
2. Authorisation to use University computer facilities and services is given on the understanding that these facilities and services are used for academic, administrative, or other specified purposes, and only by the person authorised. Modest use for non-academic purposes will be acceptable, where this does not adversely affect University operations, although the extent of such use is subject to the discretion of the Director of Academic Services. Users may not provide access details, such as passwords, for University computer facilities and services, to others.
3. No user shall attempt to access any computer facilities or services for which specific authorisation is required unless they have been given that authorisation. Use must not be made of computer resources allocated to another user.
4. No user shall by any wilful or reckless act jeopardise the integrity of any computer equipment, its associated systems programs, or any other stored information.
5. No user shall by any wilful or reckless act deny the use by other legitimate users of any computer facility or service.
6. All users shall treat as privileged any information, including software, not provided or generated by themselves which may become available to them through their use of the University computer facilities and services; they shall not copy, modify or disseminate any part of such information without explicit permission from the appropriate body.
7. No user shall introduce copyright software on to University computer facilities and services without appropriate authorisation from the Director of Academic Services, or in the case of computer facilities in the Faculties, from the Dean of Faculty.
8. All computer facilities and services users must comply with the requirements of: The Obscene Publications Act 1959, The Sex Discrimination Act 1975, The Race Relations Act 1976, The Protection of Children Act 1978, The Contempt of Court Act 1981, The Telecommunications Act 1984, The Public Order Act 1986, The Copyright, Designs and Patents Act 1988, The Computer Misuse Act 1990, The Trademarks Act 1994, The Data Protection Act 1998, and any other relevant legislation that may come into force throughout the duration of these Regulations.
9. The University computer facilities and services may not be used for commercial purposes, or for private purposes including consultancy or any other work

outside the scope of official activity, without first obtaining the written permission of the Director of Academic Services, or Dean of the appropriate Faculty. Use of University computer facilities and services for such purposes without permission may result in withdrawal of, or restriction of, access.

10. All users must abide by the University's *Guidelines for the proper use of computer facilities and services* as approved by the Director of Academic Services. Certain guidelines will be reproduced in the Student On-line Handbook. Copies of the entire guidelines will be on display in most computer rooms and available on request from Academic Services *Computing*.
11. Any user believed to be in breach of any of the Regulations listed above will be reported to the Director of Academic Services, in accordance with the University Code of Discipline.

REGULATIONS GOVERNING THE CONNECTION OF DEVICES TO THE UNIVERSITY NETWORK

This document presents the regulations of the University of Hull for the connection of computers and other devices to the University's data network. Devices include, but are not limited to, desktop computers, laptops, PDAs, servers, wireless computers, specialised equipment, cameras, environmental controls, video conferencing equipment and telephone system components.

A connection to the network is defined as any logical connection between a device and the University's network infrastructure, and includes direct, dial-in, wireless and Virtual Private Network connections. No distinction is made between personally-owned devices and those purchased by the University or its associates.

- 1 The University reserves the right to monitor traffic on the network for the purpose of protecting the integrity and performance of the network¹.
- 2 The University reserves the right immediately to disable a connection when the integrity or performance of the network is threatened or degraded by the attached device.
- 3 All devices connected to the University network must be centrally registered with IT Systems. The University reserves the right to disconnect any device using the network that has not been properly registered.
- 4 Any computer or device that has been disconnected from the network must not be reconnected until permission to do so has been granted by IT Systems.
- 5 All privately configured workstations² and servers connected to the University network must have University approved anti-virus software installed and maintained.
- 6 The operating systems and applications of privately configured workstations and servers, connected to the University network, must be maintained with the latest critical updates and patches.
- 7 A network that is not installed and operated by IT Systems is deemed to be a private network and is not allowed to be connected to the University network without written prior agreement from IT Systems.
- 8 The University reserves the right to control the quantity of bandwidth allocated to any device connected to the University network.
- 9 Peer to peer file-sharing is not permitted on the University network without written prior agreement from IT Systems.

¹ In accordance with "The Guidelines for University systems monitoring" as contained in the document *Guidelines governing the proper use of University computer facilities and services*.

² A privately configured workstation is a device that has not been configured by IT Systems or does not run the standard IT Systems desktop image.