Information Strategy

Brunel Acceptable Computer Use Policy (BACUP)

The purpose of this document is to lay forth the rules for computer use by Brunel users, whether such use is conducted on Brunel premises, using Brunel-owned machines, conducting recognised Brunel business, or interacting in any way with the Brunel network. Within this document, where such usage is unambiguous, we may refer to it by the term '[the] Acceptable Use Policy'.

August 2009

© 2009 Brunel University

Document properties

Authority

Director, Computer Centre

Sponsor

Director, Computer Centre

Responsible officer

Policy Development and Quality Manager, Computer Centre

Recent version history

Current version, August 2009, is derived from and supersedes version published in May 2007, and earlier versions.

© 2009 Brunel University

1 Introduction

1.1 Scope of conditions of use

These rules are, in part, derived from the Universities and Colleges Information Systems Association (UCISA) Model Regulations. As such they apply to use of all computers, including computing devices such as (but not limited to) personal digital assistants, in the University and to the use of the data networks of Brunel University, whether directly connected, wirelessly, by mobile telephone or by any other means. They also apply to the use of the Joint Academic NETwork (JANET) and to the use of any remote computers whether accessed via JANET or otherwise.

These conditions apply to

- all users of information and communications technology and services — staff (academic, technical, administrative and other), students, affiliate users and others.
- all types of usage of information and communications technology and services — academic, administrative and others.
- all types of information and communications technology and services — including (but not limited to) personal computers (including portable and mobile devices), workstations, server and client systems, computer networks; all software and data thereon; all computer-based information systems provided for administrative or other purposes.
- all facilities for the use of information and communications technology and services —
    - using any equipment owned, leased, hired or otherwise provided by the University.
    - using any software, etc., licensed for use by duly authorised and/or authenticated Brunel users.
    - using any equipment (irrespective of ownership or management) connected directly or remotely to the University's network or to its facilities for the use of of information and communications technology and services.
    - using any equipment for the use of information and communications technology and services while on the University's premises.
    - using any equipment for the use of information and communications technology and services while acting on behalf of the University or with any connection thereto.

Hereinafter, the term *Information and Communications Technology and Services* will be abbreviated to *ICTS*, unless by so doing, ambiguity would be created. The term *ICTS facilities* will be used to encompass all equipment, software, service, etc., which falls within the ambit of this Policy; similarly, the term *ICTS use* will be taken to encompass the use of any such ICTS facility or facilities.

Some sections apply specifically to the use of ICTS facilities provided via the University's Computer Centre. In addition, other schools or departments may have additional rules relating to the use of other ICTS facilities, whether locally-managed machines on University premises, remote machines elsewhere, or machines owned by users or third parties, and it is the user's responsibility to become familiar with these, and to abide by the set of rules formed by the consolidation of such local rules with the rules contained herein.

1.2 Disciplinary action

In the event of an apparent breach of the conditions of this Policy by a user, a group of users, or a user (or users) acting for such a group, the Director of the Computer Centre, or designated agent, has the authority to withdraw access to all or any subset of ICTS facilities from the user(s) and/or members of the group in question, or to commute such sanctions by issuing a warning of unacceptable use to the user(s) and/or members of the group in question. Failure to respond to a warning, repeated breaches or serious transgression will result in immediate withdrawal of access to computing facilities.

In the event of the withdrawal of facilities, a report will be made by the Director of the Computer Centre, or designated agent, to the user's school, department or institution. Recourse will be made to the University's usual disciplinary procedures, where it is deemed necessary by the Director of the Computer Centre. Legal action may be taken by the University where necessary.

1.3 Supervisory measures

To ensure that the standards of this Policy are maintained, the University reserves the right, as far as resources permit, to examine files, Web pages or messages, and to monitor the work of a user whose conduct gives the University reason to suspect of committing a breach of such standards.

In addition, users should note that sundry legislation (including, but not restricted to those discussed within this Policy) authorises appropriate individuals within the University to monitor and/or record some or all communications, data holdings and/or transactions for purposes specified in the relevant piece of legislation.

1.4 Currency

This Policy will be updated from time to time, and it is the responsibility of each user to maintain awareness of the current provisions of this Policy. Enquiries may be made to the Computing Support office within the Computer Centre.

 © 2009 Brunel University

2 Legal requirements

2.1 Preamble

Any infringement of the law may be subject to penalties under civil or criminal law as provided by relevant legal instruments, and such law may be invoked by the University. In particular, the following acts are relevant to computer use. The examples given below are intended as a lay guide and do not attempt to cover all eventualities. Infringement of these acts may incur sanctions or University disciplinary action instituted by the Director of the Computer Centre and/or by the University (instead of or as well as legal proceedings).

2.2 General lawful behaviour

In addition to any ICTS-specific legal duty which is set out hereunder, there is a constant and inflexible duty laid upon each user and upon any grouping of users to abide, jointly and severally as relevant, by all relevant Acts of Parliament and similar legal instruments at all times while connected (or attempting to make a connection) to the Brunel University Data Network (BUDN) — often referred to as "the Brunel network", "the University's network", etc.

2.3 Computer misuse

2.3.1 Preamble

The principal piece of legislation is the **Computer Misuse Act 1990** which secures computer material against unauthorised access or modification. A breach of this Act is a criminal offence: an individual convicted under this Act may receive an unlimited fine and a prison sentence of up to five years.

2.3.2 Categories of offence under the Computer Misuse Act 1990

2.3.2.1 Unauthorised access

It is an offence to gain access without authorisation as a preparation for a further offence, whether or not that further offence is actually committed. This would, for example, include using another user's username and password for any reason, or attempting to access another user's files without that user's express permission.

Sharing a username and password without the explicit agreement of the Computer Centre constitutes an offence by each party (whether lender or borrower).

2.3.2.2 Unauthorised access with intent

It is an offence to use a computer to gain access to any program or information which the user has no authorisation to access or use. This would, for example, include access to financial, administrative or examination-related data by unauthorised individuals.

2.3.2.3 Unauthorised modification

It is an offence to make any modification to any program, file, data, electronic mail message or other computer material belonging to another user without the permission of that user. This would, for example, include the unauthorised destruction or alteration of another user's files, the creation, introduction or forward transmission of a virus, changing examination results and deliberately generating information to cause a system malfunction.

2.3.3 Ensuring compliance

The University, exercising its duty to ensure compliance, may inspect equipment and monitor ICTS use on University premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any ICTS facilities or ICTS use to a compliant state. Furthermore, the University may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes.

2.4 Copyright, licensing and related concepts

2.4.1 Preamble

The principal piece of legislation governing copyright is the **Copyright, Design and Patents Act 1988** and its subsequent amendments. In general, copyright law gives the owner of a piece of literary or associated work (including, amongst other types of work, software, music, artistic works and photographs) the right to prevent that work from unauthorised copying. The original focus of copyright law on printed matter has long been extended to other media (for example, sound recording and performance), and recent developments have incorporated a raft of 'digital rights' within protective legislation. The concept of 'fair dealing' allows limited use of copyright works for the purposes of research, private study, criticism and review; since the 'fair dealing' test is qualitative rather than quantitative (the oft-repeated 'ten-per-cent guidance' has no general basis), the prospective user must check with the copyright owner before use.

This means that most information and software accessible via the network is subject to copyright and/or restrictions on its use. Each user must respect this copyright and must comply with any published usage restrictions relating to any program, information, image, web page or other material. Each user must treat as privileged any information (not provided or generated by himself or herself) which may become available through the use of computing facilities; no part of such information may be copied, modified, disseminated or used without the permission of the appropriate person, body or group of people.

Any user who installs software and/or information on University equipment (including remote filestore and portable/mobile devices such as laptops or personal digital assistants) must ensure full compliance with any relevant copyright and licensing requirements.

2.4.2 Software copyright

In general, software products (including systems, applications and database products) are only licensed for use on the system on which they are first installed. It is a criminal offence to make an unauthorised copy of any such product for onward distribution (even without charge); to do so for private purposes is a civil offence (against which software companies are increasingly rigorous in taking action).

No user may make a copy of software or information from or onto machines or systems within the University without first having obtained the requisite authority from the copyright holder: it is the user's responsibility to make such prior investigations of the right to copy, and to be able to present evidence thereof on demand by the Computer Centre.

 © 2009 Brunel University

2.4.3 Copyright and the internet

Material on the internet is subject to copyright in the same way that it would be in another form of publication. A webpage is a literary work (in 'as visible' and in HTML form), a text article on a webpage is a separate literary work, a graphical image on a webpage is an artistic work, and so on for other such component works. The transient copy of such works into a computer's memory is generally covered by the principles of fair dealing, but this gives no authorisation to make further copies and use of the material. The copying of Web materials to permanent storage is subject to the 'fair use' test (see below), and any comprehensive copying of a website or of a recognisable sub-unit of a website (for example, a complete subhierarchy at any lower level within a website) is likely to infringe copyright.

A user must seek and gain permission from a copyright owner before placing any copyright material on any web page, or in any document which may be retrieved electronically.

This is an area which is particularly sensitive, and which is policed vigorously by the holders of the intellectual property rights. A single infraction may lead to action by rights-holders (or their agents) which will inhibit the free flow of business throughout Brunel: it is therefore treated very seriously by the University, and it is increasingly likely that police action may ensue against transgressors.

2.4.4 Trade marks and brands

Trade marks, service marks and brand names are important assets of their owners, and many of them are registered in order to gain protection from unauthorised use. Owners have protection against unauthorised use of non-registered marks where such use is regarded as 'passing off': this practice damages the reputation of the owner through confusion as to the source of the goods or services offered under the name, mark or 'look-and-feel'. Each user has the responsibility to avoid any infringement of any such marks, and to render such marks and names in the format specified by their owners.

2.4.5 Licensed use of materials

Most software products and acquired data are restricted in their use by a licensing contract between the user and the owner. It is essential that any user is able to present, on demand at the point of use, proof of authority from the licensor to use software or data. Licences which cover the authorised use of software or data which are acquired on behalf of the University must be lodged and/or managed in accordance with relevant University procedures.

Many of the licences held by the University restrict the usage of such materials to educational use. It is the responsibility of the user to check licensing conditions before any non-educational use (whether personal, not-for-profit or commercial) is made of any product on University premises or involving the ICTS facilities of the University.

2.4.6 Fair use

In addition to simple access rights, copyright law and licence conditions contain reference to the concept of 'fair use'. It is important to realise that, as stated above, there is generally no quantitative definition. Within the context of university business, 'fair use' is easiest described as the minimum consistent with the execution of the task in hand. Excessive copying, quotation, downloading or similar activity will render the user liable to suspension for breaching this aspect of the Acceptable Use Policy.

This is an area which is particularly sensitive, and which is policed vigorously by the holders of the intellectual property rights. A single infraction may lead to action by rights-holders (or their agents) which will inhibit the free flow of business throughout Brunel: it is therefore treated very seriously by the University, and it is increasingly likely that police action may ensue against transgressors.

© 2009 Brunel University

2.4.7 Ensuring compliance

The University, exercising its duty to ensure compliance, may inspect equipment and monitor ICTS use on University premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any ICTS facilities or ICTS use to a compliant state. In this respect, the Computer Centre will work with the University's Copyright Officer and other staff. Furthermore, the University may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes.

2.5 Data protection

2.5.1 Preamble

The principal piece of legislation is the **Data Protection Act 1998**, which is concerned with the acquisition, processing, use and disclosure of personal data relating to a living individual and of information derived therefrom. The term 'personal data' is defined to encompass data which relate to a living individual who is identifiable from these data, whether on their own or in conjunction with other information (for example, by cross-referencing a questionnaire form number against mail-merge details of the recipient of that particular questionnaire form). The simple act of displaying data on a screen amounts to the 'processing' of these data under the Act.

2.5.2 Registration

Any user in possession of personal data on living individuals 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 any holdings of personal data are registered internally with the University's Office of the Secretary to Council, whose officers have the power to require modification or deletion of data in order to ensure compliance with the Act.

No student user (whether undergraduate or postgraduate, enrolled on a taught course or for a qualification by research) may construct or maintain any computer file of personal data for use in connection with their academic studies without the express authority of an appropriate member of staff. The member of staff giving such authority should make the student user aware of the Act's requirements, inform the student user of the necessity to abide by the Data Protection Principles, conduct any necessary discussions with the University's Office of the Secretary to Council in conjunction with the student user, and apprise the student user of the appropriate level of security arrangements which should be attached to a particular set of personal data.

It is important to ensure that, in addition to Data Protection law, the collection and processing of any such data conforms to the University's standards for research ethics, and it is the responsibility of the user to ensure that this is the case, by consulting with the appropriate research Ethics Officers at School or University level.

2.5.3 Principles

Personal data shall

- be obtained and processed fairly and lawfully, and shall not be processed unless certain conditions are met

 © 2009 Brunel University

- be obtained for a specific and lawful purpose, and shall not be processed in a manner incompatible with that purpose
- be adequate, relevant and not excessive for that purpose
- be accurate and kept up to date
- not be kept for longer than is necessary for that purpose
- 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 equivalent levels of protection for personal data

It should be noted that any material placed on the Web is considered to be worldwide-accessible, and therefore personal data which are made available across the Web are considered to have been transferred outwith the European Economic Area: in such a case, specific consent from the individual concerned will be a necessary prerequisite.

Users are referred to the current version of the *JISC Data Protection Code of Practice for the HE and FE Sectors*, and are advised to search for 'data protection' from the JISC homepage at **http://www.jisc.ac.uk** for the most recent publications on the subject.

2.5.4 Ensuring compliance

The University, exercising its duty to ensure compliance, may inspect equipment and monitor ICTS use on University premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any ICTS facilities or ICTS use to a compliant state. For the purposes of ensuring Data Protection compliance, the Computer Centre will work with the Records and Information Office. Furthermore, the University may use logged data, may institute the logging of data, may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes.

2.6 Defamation

2.6.1 Preamble

The principal piece of legislation is the **Defamation Act 1996**. Defamation (incorporating libel and slander) involves making a statement which would tend to lower the person (about whom the statement is being made) in the estimation of right-thinking people, or which would cause that person to be shunned or avoided. The defamation will be libellous if it is committed to a permanent form (this includes permanent electronic storage, electronic mail and the like), otherwise it is slanderous.

2.6.2 Requirements

The internet places special responsibility upon each of our users, in that electronic communications and webpages may be duplicated, transmitted and forwarded to third parties with ease. The generally less formal ethos of electronic mail, newsgroups, bulletin boards and chatrooms breeds a relaxed attitude to content, but the law is applied in exactly the same manner with the same standards and to the same effect. The use of a hyperlink to a third party's statement which is considered defamatory is considered to be tantamount to publishing the defamatory statement.

No user may hold in files (or Web pages), or transmit electronically, data which are defamatory; similarly, no user may publish a link to such data held by a third party. In this context, the user is entirely

responsible for the content of his or her files, Web pages (including hyperlinks contained thereon) and messages. Any such data received involuntarily, *e.g.*, through electronic mail, should be deleted after the appropriate staff of the Computer Centre have been notified. All users must take all reasonable steps to guard against the quotation from, or other use of such statements by third parties which might encourage an inference of a defamatory statement on the part of any Brunel user.

2.6.3 Ensuring compliance

The University, exercising its duty to ensure compliance, may inspect equipment and monitor ICTS use on University premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any ICTS facilities or ICTS use to a compliant state. Furthermore, the University may use logged data, may institute the logging of data, may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes.

2.7 Obscene and offensive publication

2.7.1 Preamble

The principal pieces of legislation are

- **Obscene Publications Act 1959**
- **Obscene Publications Act 1964**
- **Protection of Children Act 1978**
- **Criminal Justice and Public Order Act 1994** (which also amends certain provision of the above Acts)
- **Telecommunications Act 1984**

The law gives a certain level of immunity to technical investigators, but only under closely regulated conditions and by explicit authority of the Director of the Computer Centre. No user may employ the defence of technical investigation without such authority.

2.7.2 Obscenity

It should be noted that the definition of 'obscene material' is not restricted to the depiction or description of sexual acts, but applies more generally to (*inter alia*) depiction or description of violence, or of drug usage in a manner which might imply advocacy.

It is an offence to distribute, circulate, sell, give, lend, let on hire, offer for sale, show, play, project or (where the matter is stored electronically) transmit obscene material. It is also an offence to transmit or store electronically data which, on resolution to a user-readable form, is obscene.

No user may hold in files (or Web pages), or transmit electronically, data which constitutes obscene material. In this context, the user is entirely responsible for the content of his or her files, Web pages and messages. Any such data received involuntarily, *e.g.*, through electronic mail, should be deleted after the appropriate staff of the Computer Centre have been notified.

2.7.3 Protection of children

The **Protection of Children Act 1978** (as amended) deals with photographic representation (including pseudophotographs and data stored electronically or on disk which are capable of conversion into a

 © 2009 Brunel University

photographic representation) of children under the age of sixteen, and of persons who appear to be under the age of sixteen. It is an offence to possess, take, make, permit to be taken, distribute (or intend to distribute), show (or intend to show), publish or have published an indecent photographic representation of such children and persons.

No user may hold in files (or Web pages), or transmit electronically, data which constitutes indecent material of this nature. In this context, the user is entirely responsible for the content of his or her files, Web pages and messages. Any such data received involuntarily, *e.g.*, through electronic mail, should be deleted after the appropriate staff of the Computer Centre have been notified.

2.7.4 Ensuring compliance

The University, exercising its duty to ensure compliance, may inspect equipment and monitor ICTS use on University premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any ICTS facilities or ICTS use to a compliant state. Furthermore, the University may use logged data, may institute the logging of data, may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes. Due to the severity of this subject, any such quarantining of assets may be very wide-ranging.

2.8 Discrimination

2.8.1 Preamble

The principal pieces of legislation are

- **Sex Discrimination Act 1975**
- **Race Relations Act 1976**
- **Disability Discrimination Act 1995**
- **Public Order Act 1986**

The first three of these Acts operate under the principle of the prevention of unfair discrimination, while the last may come into play in relation to criminal liability in internet-related matters. In addition, European Union legislation on other forms of discrimination may come into play in regard of possible discrimination of other kinds.

2.8.2 Requirements

No user may hold in files (or Web pages), or transmit electronically, data which constitutes material which may be considered discriminatory on the grounds of gender, sexual orientation, disability, race or ethnic origin. In this context, the user is entirely responsible for the content of his or her files, Web pages and messages. Any such data received involuntarily, *e.g.*, through electronic mail, should be deleted after the appropriate staff of the Computer Centre have been notified.

2.8.3 Ensuring compliance

The University, exercising its duty to ensure compliance, may inspect equipment and monitor ICTS use on University premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any ICTS facilities or ICTS use to a compliant state. Furthermore, the University may use logged data, may institute the logging of data, may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes.

2.9 Official and trade secrets

2.9.1 Preamble

The confidentiality of information which has been obtained by agreement with third parties, or which has been obtained in the course of work undertaken as part of an agreement with third parties, is covered by the contractual details of the agreement. No user may hold in files (or Web pages), or transmit electronically, data which contravene the provisions of any such agreement.

2.9.2 Trade secrets

The use of data in research or other work undertaken in conjunction with a commercial partner must respect the commercial confidentiality of information gained in the course of such work. A contract with such a partner will place appropriate restrictions on the use of data, and it is the responsibility of the user to ensure that the conditions within the contract are observed scrupulously.

2.9.3 Official secrets

The handling of information which is covered by the **Official Secrets Acts 1911-1989** is subject to stringent restrictions and procedures. A user must gain specific authority from the Director of the Computer Centre prior to the storage, use or accessing of any information covered by the provisions of the United Kingdom's Official Secrets legislation, or by the provisions of similar legislation of another country.

2.9.4 Ensuring compliance

The University, exercising its duty to ensure compliance, may inspect equipment and monitor ICTS use on University premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any ICTS facilities or ICTS use to a compliant state. Furthermore, the University may use logged data, may institute the logging of data, may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes.

2.10 International ramifications

2.10.1 Preamble

The international nature of the internet makes it necessary that users consider the laws applicable in separate jurisdictions. Materials which are legal in the country of origin are still subject to local legislation when they are received, distributed, used or otherwise pass through another country. Thus any materials communicated to a machine on Brunel premises become subject to English law in respect of their use or consumption within this country, and any materials which originate at Brunel will be liable (as regards the provision) to legislation in the countries of use or consumption.

2.10.2 Requirements

Each user has the responsibility to ensure compliance with all relevant legislation under English law in relation to his/her use or consumption of materials communicated to the data network of the University or to machines owned by the University or on University premises from other jurisdictions.

 © 2009 Brunel University

Each user has the responsibility to ensure compliance with all relevant legislation in the countries of use or consumption of materials communicated by him/her thereto from the data network of the University or from machines owned by the University or on University premises.

2.10.3 Ensuring compliance

The University, exercising its duty to ensure compliance, may inspect equipment and monitor ICTS use on University premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any ICTS facilities or ICTS use to a compliant state. Furthermore, the University may use logged data, may institute the logging of data, may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes.

2.11 Investigatory powers

2.11.1 Preamble

The principal piece of legislation is the **Regulation of Investigatory Powers Act 2000**: pursuant to that Act, the **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** are relevant to investigations and interception of communications within the University. In general, the Act makes it an offence for any person, without lawful authority, to intercept any communication which is transmitted on a public or private telecommunication system, and outlines specific authorities for such interception.

Any such interception must be undertaken under due authority from the appropriate senior officer of the University.

2.11.2 Authorised purposes

Duly authorised members of the University may monitor or record all communications transmitted on the data network of the University in order to

- establish the existence of facts under dispute (for example, to find the authority for an extension to a deadline)
- ascertain compliance with this Policy
- ascertain or demonstrate the standards of achievement of users of the ICTS facilities of the University (for example, in the use of computer-assisted assessment)
- prevent or detect crime
- investigate or detect unauthorised ICTS use
- ensure the effective use of the ICTS facilities of the University (for example, the monitoring of system traffic and the storing of information about such traffic for statistical and forecasting analysis)

In addition, duly authorised members of the University may monitor communications to a user and files held by a user for purposes relating to the continuity of the University's business (for example, to check for business-related electronic mail during a user's absence due to sickness or holidays). Such activity is subject to a process of due authorisation, involving the Head of School (or equivalent unit of the University) and the Director of Human Resources (or Head of Registry, in the case of a student account).

No user may intercept any communication on the BUDN without due authorisation by the University: in order to seek such authority, a user must in the first instance make an application to the Director of the Computer Centre or designated agent. Each user who makes such an application must satisfy the University that the interceptive activity in question does not contravene the provisions of the European Convention on Human Rights, as enacted into British legislation by the **Human Rights Act 1998**.

2.12 Legal responsibility/liability disclaimer

The University accepts no responsibility for the malfunctioning of any facility of the Computer Centre, or of any part thereof, whether hardware, software or other.

The Computer Centre will follow recognised codes of practice concerning the archiving of magnetic disk files and the security of magnetic disks, tapes and other media, but will not take responsibility for the security of an individual's computer files. Users are advised to ensure that they, by acting independently, maintain adequate backup copies and/or file printouts of any data they wish to retain.

The Computer Centre does not operate a high security system and cannot give any warranty or undertaking about the security or confidentiality of data or other material submitted to or processed by the Computer Centre or otherwise deposited or left in areas owned or managed by the Computer Centre. Use of encryption is possible but a user with an intercepted encrypted file or message may be instructed to de-crypt it for inspection to maintain the standards of the Acceptable Use Policy.

Where necessary (for example, for housekeeping purposes) the Computer Centre reserves the right to compress, archive to tape or other media, or otherwise remove files stored on central filestore by existing or past users. Such activity will be carried out in accordance with the retention schedule of the University's Records Management Policy, and with appropriate data managemnet legislation.

No claim shall be made against the University, its employees or agents in respect of any loss alleged to have been caused whether by defect in the resources or by act or neglect of the University, its employees or agents.

 © 2009 Brunel University

3 Contractual responsibilities

3.1 Joint Academic Network Acceptable Use Policy

Each member of the University must abide by the Joint Academic Network Acceptable Use Policy. This Policy may be viewed via the World Wide Web at

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

3.2 EduServ Code of Conduct

Each member of the University must abide by the EduServ Code of Conduct for the use of software or datasets issued by them. This Code of Conduct may be viewed via the World Wide Web at

http://www.chest.ac.uk/conduct.html

3.3 Use of facilities at other institutions

Users must only use any other computing IT facility with the permission of the designated authority for that IT facility. Users of networks and remote IT facilities shall obey any published rules for their use. Users shall observe the level of authorisation and resource they are granted at remote IT facilities.

4 User authorisation

4.1 Registration

4.1.1 Scope

No persons or persons shall use the central computing facilities without due authorisation being given and registration completed.

All members and employees of the University shall normally be entitled to such authorisation in pursuance of their proper University work.

Others may be permitted registration according to circumstances, and this may involve charges for use of facilities.

4.1.2 Means of registration

Requests for registration should in the first instance be directed to the local Computing Support office.

External users from other higher education institutions should bring an accompanying letter from their department head or equivalent supporting their request for use of the Brunel facilities as well as some current university/college identification. The decision to grant, limit or refuse access lies within the power of the Director of the Computer Centre or his designated agent.

4.1.3 Responsibility

Every allocation of computing resources shall be authorised on the understanding that it is to be used only for the purpose for which it was requested, and only by the person or persons on whose behalf the request was granted. No authorised user shall allow use of his or her own username and password by any other persons, nor make use of any other user's username and password.

The facilities may only be used for genuine academic or related purposes. For any other use, special rules will apply and clearance must be obtained from the Director of the Computer Centre before any commitments are made to external sponsors. These special rules will cover, *inter alia*, payments due to the University for the use of its equipment, will prevent license infringements, and will protect the University from any claims for damages, etc. which may arise from such use.

Permission to use central computing resources is given to students for the purposes of *bona fide* University work, such work being authorised and supervised by a responsible member of staff of the University. Work carried out in fulfilment of course requirements meets this condition; other work within these purposes is permitted only subject to its being authorised by and supervised by a member of staff.

Any personal, not-for-profit or commercial exploitation of university computing resources — if permitted at all — will be strictly controlled. In particular, personal off-campus accounts must be used for correspondence and personal business which does not meet the consitions of *bona fide* Brunel business as outlined above. Normally, commercial exploitation by staff, students or others will violate the terms under which much equipment is purchased, and will break the conditions of most software licenses. Such use which impinges on the central service — even as minimally as using a networked printer — may cause infringements which could render the University liable to prosecution. Personal or group solicitation on behalf of third parties, whether commercial, non-profit, political or charitable, is similarly beyond the

 © 2009 Brunel University

scope of acceptable use of a Brunel account. Any user contemplating such personal, not-for-profit or commercial use must, therefore, contact the Director of the Computer Centre in advance to seek consent.

Authorised users are required to inform the Computer Centre of a change of status (for example from student to staff, or on departure from the University): this requirement is waived for the notification of completion of an approved period of study by a taught student.

All work carried out on central computing facilities is deemed to be the property of the University. As such, the Computer Centre will meet formal requests from a University department for retrieval of files belonging to existing or past staff or student members of that department.

4.2 Charging

Any person or persons to whom chargeable computing resources have been allocated (for example, for consultancy or other work outside official duties) or chargeable services provided (for example, software installation or hardcopy output, including laser printout) shall be personally responsible for reimbursing the University by a specified date, at the rate agreed in advance with the Computer Centre.

Failure to make such reimbursement will normally result in immediate withdrawal of access to the facilities until full settlement is made.

5 Behaviour

Users of computing facilities should always act with consideration and respect for the staff, other users and the equipment provided — hardware, software, fittings and furniture.

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 and related purposes, or for other special purposes for which express and explicit consent has been obtained from the Computer Centre.

Users need to be responsible in their use of

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

Irresponsible use wastes these resources and includes, for example,

- the collection, creation, storing, display, production and circulation of offensive, abusive or pornographic material in any form or on any University equipment.
- the abuse of electronic mail and similar messaging facilities, such as the sending of pornographic, chain, junk or bulk mail. If you receive any mail of these types, please forward it to the Computing Support staff who will deal with it on your behalf.
- the playing of any kind of game at any time (with the specific exception of duly authorised academic activity essential to curricular activity within certain degree programmes).
- excessive use of multi-user chat programs (for example, IRC).
- a refusal to vacate a PC/workstation in a public-access workarea if you have finished using it for coursework when there are queues for their use.
- locking access to a PC/workstation in a public-access workarea at any time
- leaving a PC/workstation logged in while unattended (even for a short time) in a public-access workarea

Any of the above constitutes a serious infraction of the Brunel Acceptable Computer Use Policy and you will be subject to the disciplinary procedures set out in this Policy.

 © 2009 Brunel University

Advice on proper use of software and hardware is given in the documentation published (in hardcopy and/or in electronic form) by the Computer Centre. If in doubt, please ask first. You may make enquiries by contacting the Computing Support team in any of the following ways.

- By electronic mail to **computing–support@brunel.ac.uk**
- By telephoning 01895-265888 or internal extension 65888
- By facsimile transmission to 01895-252691
- In person to room 031 in the John Crank building

In addition to avoiding the waste of computing resources, users must respect the supply of consumable items; particularly with printed output, both avoiding excessive output of their own and treating that of others with consideration.

5.2 Damage and fault reports

The University computing facilities are provided for common usage, and all users need to take reasonable steps to avoid damage or prolonged loss of service. Damage refers to any deliberate or accidental damage to any IT facility or University property including any modifications to hardware or software, which incur time or cost in restoring the system to its original state.

Users must not cause any form of damage to the University's IT facilities, nor to any accommodation or service related to them.

Installation (or modification of the setup) of software, or connection of hardware (including peripherals) to the Brunel University Data Network (whether directly or via another machine) must be with the explicit approval of the Director of the Computer Centre and in accordance with all local codes of practice.

Users should also take all reasonable steps to report any faulty equipment to the Computer Centre, and endeavour to leave computers in a clean, usable state. In particular, users must neither smoke, eat nor drink in or within a ten-metre adjacency of any public room or area (whether workarea, corridor or other location), or any free-standing asset (such as a print station or kiosk machine) owned or managed by the Computer Centre.

5.3 Health and safety

In the event of a fire alarm's being sounded, or in any other emergency, all computer users and visitors will immediately leave the area and proceed to the appropriate assembly point, as indicated on notices and/or directions within the area. No person shall re-enter the evacuated area until authority is given by the senior incident officer on site.

Users must ensure that access to computing areas, and to machines within those areas, is kept clear for any user. Bags and coats, chairs and other furniture should be kept clear of gangways, fire exits and other access routes, and rooms must be kept within their capacity and not overcrowded. A maximum room capacity of two persons per workstation/PC contained therein will normally be permitted: local notices will inform users of any divergence from this norm.

Users must not disconnect machines, nor attempt to repair damage or faults to any machine. Please report any fault or damage to computing equipment in one of the following ways.

- By electronic mail to **computing–support@brunel.ac.uk**

- By telephoning 01895-265888 or internal extension 65888
- In person to room 031 in the John Crank building

Dispose of rubbish, including waste paper, in the appropriate receptacles.

Children under the age of 17, other than those with an explicit and express invitation from the Director of the Computer Centre, are not permitted in any room or area owned or managed by the Computer Centre, nor is any animal (with the exception of a service dog in the course of its work, accompanied by its responsible person).

No unauthorised persons should be in any workarea or similar room or area owned or managed by the Computer Centre. The authority of a member of the University to be present in a public area owned or managed by the Computer Centre will include (but will not necessarily be restricted to) the carrying and the display on request of a current and valid Brunel University identity card: anyone who is unable to provide such a card for inspection at the time of request may be required to vacate the area.

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

5.4 Information security

The security of the University's network against unauthorised use and access must be a primary concern of each and every user at all times. It is a clear breach of this Policy to act with disregard, whether wilful or negligent, for best practices of information security, and such disregard may lead to the institution of disciplinary proceedings against any transgressor.

The connection of devices to the University network must always be made in accordance with the current rules of the Computer Centre. These rules cover, but are not limited to, the acceptable level of protection against viruses, worms and other such nuisances. It is the user's responsibility to confirm current requirements before attempting to connect any machine which does not enjoy the University's standard PC image (whether that machine is University property, or is owned by the user or a third party.

Malicious content may lurk on, or be transferible from web content, electronic mail or analogous media. It is a breach of this Policy to facilitate, whether deliberately or through negligence, the transfer of such material onto the University network, or onto any machine connected thereto. Equally, it is a breach of this Policy to facilitate the transmission of such material to other sites from or via the University network. This includes the handling of any electronic mail suspected of the potential to contain such material, whether by explicit sending, automated redirection or the simple act of browsing the content. It also includes the proliferation by any means of spam and phishing messages.

5.5 Reputational damage

Consequent on any breach of information security as instanced above, or following any instance of poor online behaviour by a Brunel account-holder or attributable to a Brunel-managed entity on the internet (for example, an IP address assigned to Brunel), there is a risk of reputational damage to Brunel. this may include automated or manual inhibition of service to and from Brunel, the invocation or creation of penalty clauses within contracts, or general deprecation of Brunel within the internet citizenry. Such reputational damage hurts Brunel seriously, quickly, and potentially for a long period of time. The endangerment of Brunel's online reputation is a serious breach of this Policy, and disciplinary proceddings may be instituted against any user who, whether deliberately or negligently, exposes the University to such risk.

 © 2009 Brunel University

5.6 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.

In particular, avoid disturbance of others by noise, including but not exclusively

- mobile telephones — see below
- personal entertainment systems
- playing of sound bites

or other interruptions (such as group activities). Conversation must be kept to an absolute minimum, in length and in volume. If you may be heard above normal keyboard noise in the room, you are too loud.

Mobile telephones cause major disruption in computer workareas and adjacent locations. For this reason,

- audible ringers must be switched off while in premises owned or managed by the Computer Centre
- you must vacate premises owned or managed by the Computer Centre before making or taking a call, and you must logout from any PC or workstation before doing so

Ensure machines are left available to others when leaving a computer for a break (however short), by logging out. This will protect your work as much as helping other users. It is an offence against this Acceptable Use Policy for any user to lock access to any PC or workstation in any public-access workarea, kiosk location, or similar facility, or to leave such a device unattended while logged in. Staff of the Computer Centre, and their duly authorised agents, have the authority to close any unattended session on any PC or workstation in a public-access workarea, kiosk location, or similar facility.

Often, a computer workarea is booked for teaching purposes and sometimes this leaves machines in these areas unused. You may be allowed access to one of these machines but this will be only with the consent of the staff member(s) in charge of the booked session. Staff running such booked sessions must remain aware of the demand for PC/workstations and, unless there are over-riding considerations (such as the need for security of a session being undertaken under examination conditions), should allow access to any unused machines. If you are allowed access to a spare machine during a booked session, you should display appropriate behaviour (*i.e.*, by respecting the primacy of the booked session, by making no noise and by remaining as unobtrusive as possible). If you prove to be a distraction to participants of the booked session, you will be asked to leave by the staff member(s) in charge of the booked session, and you should do so without question or argument and with a minimum of disturbance.

Observe opening and closing times, leaving promptly when requested for booked sessions or closure. Do not congregate near a facility prior to its advertised opening time or in advance of the ending of a booked session, nor while waiting for the availability of a service (*e.g.*, the availability of a PC or a public-service printstation).