Brunel Legislative and Regulatory Framework Policy

Brunel University London

An ISO/IEC 27001:2013: Aligned Document - Implementing Cyber and Information Security Best Practice

Internal Use Only

Mick Jenkins
Chief Information Security officer

Document History

Version	Author	Comments	Date
V0.1	Iain Liddell	Brunel Acceptable Use Policy	20/06/2015
V 1.0	Andrew Clarke	Initial Draft (from BACUP) / GDPR	06/04/2018
V 1.1	Andrew Clarke	Format changes Strategy & Governance	03/05/2018
V1.2	Andrew Clarke	Replace DPA 1998 with DPA 2018	06/06/2018
V1.3	Andrew Clarke	Reference University Data Protection Policy	18/07/2018
V1.4	Andrew Clarke	CISA approval (duplicate text removed)	07/09/2018

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

The purpose of this framework is to clarify the legislative and regulatory framework and expectations for the acceptable use of IS resources within Brunel University London by each user to pursue their professional and academic activities.

Please refer to Brunel University London ISMS Document *BUL-GLOS-000 - SyOPs Glossary of Terms* for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Cyber & Information Security Manager	Is responsible for maintaining the acceptable use policy and to ensure that the Policy continues best practice and ensuring compliance with legislative and regulatory requirements.
All Users	It is the responsibility of all users of the Brunel University London's IS services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A8 – Asset Management
ISO 27001:2013 Conformance Control	Information Classification Objective A.8.1.3 Acceptable use of assets

1.4 Scope

This Framework is, in part, derived from the Universities and Colleges Information Systems Association (UCISA) Model Regulations, and have been amended to meet the requirements of Brunel University London. As such they apply to use of all computers, including devices such as (but not limited to) desktop, portable and mobile computers, smartphones and personal digital assistants, in the University

and to the use of the data networks of Brunel University London, 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, alumni, affiliate users and others
- all uses 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 Brunel University London
    - using any software, etc., licensed for use by duly authorised and/or authenticated users of Brunel University London
    - using any account provided by Brunel University London for any purpose, including any such account managed on behalf of Brunel University London by a third party
    - 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 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 Brunel University London or with any connection thereto

Some sections apply specifically to the use of Information Services (IS) facilities, however, colleges, departments and other units of the University may have additional rules relating to the use of other IT 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 a third party.

1.5 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 CISO, or designated agent, has the authority to withdraw access to all or any subset of IS 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 CISO, or designated agent, to the user's college, department, similar unit of the University or relevant external body, except that in the case of an alumnus/a, the CISO (or a duly designated agent thereof) will have direct authority to suspend or delete any or all access privileges. Recourse will be made to the University's usual disciplinary procedures, where it is deemed necessary by the CISO. Legal action may be taken by Brunel University London in any instance wherein it is deemed to be in the interests of the University to do so.

1.6 Supervisory measures

To ensure that the standards of this Policy are maintained, Brunel University London 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.

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 relevant legislation.

2.0 Legal Framework

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 Brunel University London. 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 CISO and/or by the University (instead of or as well as legal proceedings).

General lawful behaviour

In addition to any IS-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 and regulatory instruments at all times while connected (or attempting to make a connection) to Brunel University London's Data Network.

2.1 Computer misuse

2.1.1 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, and any individual convicted under this Act may receive an unlimited fine, and a prison sentence of up to five years.

2.1.2 Categories of offence under the Computer Misuse Act 1990

2.1.2.1 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 Brunel University London username and password without the explicit agreement of the Information Services constitutes an offence by each party (whether lender or borrower).

2.1.2.2 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.

2.1.2.3 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.

2.1.3 Ensuring compliance

Brunel University London, exercising its duty to ensure compliance, may inspect equipment and monitor IS use on Brunel University London premises, equipment or facilities, including any such facility managed on behalf of the University by a third party, and may require appropriate modification or removal of computer material to recover any IS facilities or IS 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.

2.2 Copyright, licensing and related concepts

2.2.1 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 Brunel University London equipment (including remote file store and portable/mobile devices such as

laptops or personal digital assistants) must ensure full compliance with any relevant copyright and licensing requirements.

2.2.2 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 Brunel University London 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 Information Services.

2.2.3 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 University London: it is therefore treated very seriously by the University, and it is increasingly likely that police action may ensue against transgressors.

2.2.4 Trademarks and brands

Trademarks, 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.

2.2.5 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 Brunel University London must be lodged and/or managed in accordance with relevant Brunel University London procedures.

Many of the licences held by Brunel University London 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 Brunel University London premises or involving the IS facilities of Brunel University London.

2.2.6 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 Brunel 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 University London: it is therefore treated very seriously by the University, and it is increasingly likely that police action may ensue against transgressors.

2.2.7 Ensuring compliance

Brunel University London, exercising its duty to ensure compliance, may inspect equipment and monitor IT use on Brunel University London premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any IS facilities or IS use to a compliant state. In this respect, the Information Services will work with the University's Copyright Officer and other

staff. Furthermore, Brunel University London may retain certified true copies of any data, and may quarantine equipment, for any necessary evidential purposes.

2.3 Data protection

REF. University Data protection Policy

2.3.1 Preamble

The principal piece of legislation is the **Data Protection Act 2018** which supersedes the Data Protection Act 1998, and is the UK legislation based upon the **General Data Protection Regulation** which applies in the UK from May 2018. This legislation 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 Regulation.

2.3.2 Registration

Any user in possession of personal data on living individuals must comply with the Data Protection Principles 1 – 6 of the **Data Protection Act 2018** and with any restrictions imposed to ensure adherence to the University's registration under the Regulation.

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 at foundation/preparatory, undergraduate or postgraduate level, enrolled on a taught course or for a qualification by research) may construct or maintain any computer file for 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 Regulations requirements, inform the student user of the necessity to abide by the Data Protection Principles 1 – 6 of the **Data Protection Act 2018**, conduct any necessary discussions with Brunel University London's Governance, Information and Legal Office 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 Research Ethics Officers at all appropriate levels and within all appropriate units of the University.

2.3.3 The Data Protection Principles 1 – 6 of the **Data Protection Act 2018** requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

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 outside 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.

2.3.4 Ensuring compliance

Brunel University London, exercising its duty to ensure compliance, may inspect equipment and monitor IS use on Brunel University London premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any IS facilities or IS use to a compliant state. For the purposes of ensuring **General Data Protection Regulation** compliance, the Information

Services will work with the Governance, Information and Legal Office of the University. Furthermore, Brunel University London 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.

2.4 Defamation

2.4.1 Preamble

The principal piece of legislation is the **Defamation Act 1996**. Defamation, which incorporates 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.

2.4.2 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 email, blogs, twitter, newsgroups, bulletin boards, chatrooms and other social media 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 Information Services 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 user who is a part of, or associated with, Brunel University London.

2.4.3 Ensuring compliance

Brunel University London, exercising its duty to ensure compliance, may inspect equipment and monitor IS use on Brunel University London premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any IS facilities or IS use to a compliant state. Furthermore, Brunel University London 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.

2.5 Obscene and offensive publication

2.5.1 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 CISO. No user may employ the defence of technical investigation without such prior authority.

2.5.2 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 Information Services have been notified, in accordance with instructions given by the Information Services.

2.5.3 Protection of children

The **Protection of Children Act 1978** (as amended) deals with photographic representation (including pseudo-photographs and data stored electronically or on disk which are capable of conversion into a 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 Information Services have been notified, in accordance with instructions given by the Information Services.

2.5.4 Ensuring compliance

Brunel University London, exercising its duty to ensure compliance, may inspect equipment and monitor IS use on Brunel University London premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any IS facilities or IS use to a compliant state. Furthermore, Brunel University London 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.

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

2.6 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 CIO 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.

2.6.1 Ensuring compliance

Brunel University London, exercising its duty to ensure compliance, may inspect equipment and monitor IS use on Brunel University London premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any IS facilities or IS use to a compliant state. Furthermore, Brunel University London 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 Counter-terrorism

2.7.1 Preamble

The principal legal instrument is the **Counter-terrorism and Security Act 2015**. Brunel University London, in common with all similar bodies, must comply with the

provisions of this Act. There are several areas of operation, including (but not limited to) freedom of expression, event management, and equality, as well as the safety and security of all — staff, students and visitors — who may be present on campus and wherever people gather under the auspices of Brunel University London.

Part 5 of the Act deals with the need to prevent individuals from being drawn into terrorism, and this is a crucial part of the legislation as it affects universities.

2.7.2 Requirements

The Government has published its *Prevent* strategy (as part of the overall counter-terrorism strategy *CONTEST*) and gives guidelines on achieving its strategic objectives. Though there are no new specific duties laid upon the University, the required risk-based approach will necessitate, in some instances, stronger application and auditing of existing functions and procedures. Considering the specifics of duty aligned with the provision and use of IS facilities, these requirements will incorporate the existing filtering of mail and website access, and may also incorporate monitoring and alerting mechanisms on other software.

2.7.3 Ensuring compliance

Brunel University London, exercising its duty to ensure compliance, may inspect equipment and monitor IS use on Brunel University London premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any IS facilities or IS use to a compliant state. Furthermore, Brunel University London 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.

The University's policies relating to research ethics and allied subjects will be used to inform IS compliance in relation to topics of research which fall within the scope of the Act and its component strategies, and to the management of data connected with such research.

2.7.4 Balancing legislative requirements

The duty placed upon the University by this legislation must be carried out in compliance with other legislation, and this will necessitate a balanced and proportional response. Indeed the Act gives a nod to risk-based proportionality. The principal areas of legislative balance will be in data privacy and human rights, and the University will be assiduous in achieving a proper balance, seeking and taking account of professional guidance as necessary.

2.8 International ramifications

2.8.1 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 University London premises become subject to English law in respect of their use or consumption within this country, and any materials which originate at Brunel University London will be liable (as regards the provision) to legislation in the countries of use or consumption.

2.8.2 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 Brunel University London, or to machines owned by Brunel University London, or on Brunel University London premises, from other jurisdictions.

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 Brunel University London, or from machines owned by Brunel University London, or on Brunel University London premises.

2.8.3 Ensuring compliance

Brunel University London, exercising its duty to ensure compliance, may inspect equipment and monitor IS use on Brunel University London premises, equipment or facilities, and may require appropriate modification or removal of computer material to recover any IS facilities or IS use to a compliant state. Furthermore, Brunel University London 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 Investigatory powers

2.9.1 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 Brunel University London.

2.9.2 Authorised purposes

Duly authorised members of Brunel University London may monitor or record all communications transmitted on the data network of Brunel University London 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 IS facilities of Brunel University London (for example, in the use of computer-assisted assessment)
- prevent or detect crime
- investigate or detect unauthorised IS use
- ensure the effective use of the IS 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 Brunel University London 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 senior officer of the relevant 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 data network of Brunel University London, or on any IS facility managed on behalf of the University by any third party. Without due authorisation by Brunel University London: in order to seek such authority, a user must in the first instance make an application to the CISO or designated agent. Each user who makes such an application must satisfy Brunel University London 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**.

In the case of any such behaviour by an alumnus/a, the Director of External Affairs and the Director of the Information Services will exercise joint authority for any activity under this section.

2.10 Legal responsibility/liability disclaimer

Brunel University London accepts no responsibility for the malfunctioning of any facility of the Information Services, or of any part thereof, whether hardware, software or other, or of any IS facility managed by another unit of the University, or on behalf of Brunel University London by any third party. Information Services will follow recognised codes of practice concerning the archiving of magnetic disk files and the security of magnetic disks, tapes and other media, but 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.

Information Services does not operate a high security system and cannot give any warranty or undertaking about the security or confidentiality of data or other material submitted to or processed by Information Services or otherwise deposited or left in areas owned or managed by Information Services. 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) Information Services reserves the right to compress, archive to tape or other media, or otherwise remove files stored on central file store by existing or past users. Such activity will be carried out in accordance with the retention schedule of Brunel University London's Records Management Policy, and with appropriate data management legislation.

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

3.0 Contractual responsibilities

3.1 Joint Academic Network (JANET) Acceptable Use Policy

Each member of Brunel University London must abide by the Joint Academic Network (JANET)

Acceptable Use Policy.

3.2 EduServ Code of Conduct

Each member of Brunel University London must abide by the EduServ *Code of Conduct* for the use of software or datasets issued by them.

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.

3.4 Use of facilities managed by third parties

When using a facility provided by Brunel University London but managed on behalf of the University by a third party, the user must be bound by such rules, policies, terms and conditions applied by Brunel University London and by the third party.

4.0 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 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

- by electronic mail to **computing–support@brunel.ac.uk**
- by telephoning 01895-265888 or internal extension 65888
- in person to the Information Services Service Desk

Each user must dispose of all 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 Information Services, are not permitted in any

room or area owned or managed by Information Services, 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 work area or similar room or area owned or managed by the Information Services. The authority of a member of the University to be present in a public area owned or managed by the Information Services will include (but will not necessarily be restricted to) the carrying and the display on request of a current and valid Brunel University London 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, no user must ever act in a manner which could jeopardise the safety of himself/herself, or that of any other person.