



# Information Strategy

## Network account policy

The purpose of this document is to lay forth the policy which regulates the use of a network computer account within Brunel University London, or such an account granted by Brunel University London for use in conjunction with a facility managed on behalf of Brunel University London by a third party. It should be clear that policy is not immutable: in particular, in a field such as this, where emerging technology is interwoven with emerging law, we must be able to react to changes. In the formulation and continuous reformulation of policy, we must be guided by advice from within Brunel University London and beyond, taking due consideration of legal precedent, and having due regard to the practices and experiences of our colleagues in other institutions.

**July 2015**

---

## Document properties

### Authority

Director, Computer Centre

### Sponsor

Director, Computer Centre

### Responsible officer

Assistant Director (Governance and Corporate Services), Computer Centre

### Version history

1	1 June 2006	New document
2	7 August 2009	Comprehensive revision and updating
3	24 May 2012	Comprehensive revision and updating
4	14 February 2014	Incorporation of third-party action on behalf of Brunel
5	28 August 2014	General updating and rebranding
6	17 February 2015	Details of account review procedures added (version history updated 23 March 2015)
7	20 July 2015	Update, adding duties under Counter-terrorism and Security Act 2015

---

# 1 Introduction

## 1.1 Nomenclature

Hereinafter, where such usage is unambiguous, we may refer to key entities in concise form, *e.g.*,

- *[the] Acceptable Use Policy* for Brunel Acceptable Computer Use Policy.
- *the University* for Brunel University London.
- *ICTS* for Information and Communications Technology and Services.
- *ICTS facilities* to encompass all equipment, software, service, etc., which may fall within the ambit of this Policy.
- *ICTS use* to encompass the use of any such ICTS facility or facilities

Readers should note the convention that the word ‘university’, when presented in lower case, is a generic term referring to an unspecified qualifying institution.

## 1.2 Scope

Brunel University London must clarify how any network computer account granted by the University should be used and managed by the account-holder, whether he/she be a student, member of staff, alumnus/a, or other affiliated person, and whether the facility enjoyed by the account-holder is located at Brunel University London or is managed on behalf of Brunel University London by a third party. Each user must abide by all relevant external and internal regulations, and must act in the overall interest of the entire user community at all times. There must be clear divisions of responsibility and privileges, with the legitimate academic and corporate business of Brunel University London, and the assurance of its continuity, having due primacy.

This Policy sets out the accepted management of accounts on Brunel University London’s networked computers by all partners in the enterprise — staff, students and other account-holders. Specific reference to technical investigation ensures fairness and best practice in an area of operation which may be seen as highly sensitive. In conjunction with our guidelines of good computing practice, this Policy will enshrine general principles and practices of good management. Furthermore, it will help to ensure that Brunel University London is compliant with all relevant legislation, and that it adheres to the Seven Principles of Public Life in the United Kingdom (popularly known as the Nolan Principles)<sup>1</sup> and to high standards of ethical value, in its management of network computer accounts.

---

<sup>1</sup> See, for example, <http://www.archive.official-documents.co.uk/document/parlment/nolan/nolan.htm>

---

## 2 Supervening policies and frameworks

This policy describes the local rules by which Brunel University London business is transacted using a network account, but such use must also comply with relevant laws, regulatory instruments, policies and frameworks which operate at higher levels.

### 2.1 Brunel Acceptable Computer Use Policy (BACUP)

All computer use which takes place on, or routes activity through, the Brunel University London data network, or which uses network account privileges granted by Brunel University London for use in conjunction with facilities managed by Brunel University London, or managed on behalf of Brunel University London by a third party, is subject to the provisions of the Brunel Acceptable Computer Use Policy (BACUP). The current text of BACUP is co-located with other such documents at <http://www.brunel.ac.uk/life/study/computer-centre/policies/> and is contained within the Student Handbook. This forms part of the rules of Brunel University London.

### 2.2 Joint Academic Network (JANET)

Brunel University London's access to the Internet is regulated by the Acceptable Use Policy of the [United Kingdom] Joint Academic Network (JANET)<sup>2</sup>. This limits the use to which the access from the University to the internet beyond may be put — this obviously includes our use of network access beyond Brunel University London. Any breach of this policy jeopardises our ability to use the internet, and local sanctions will be applied with vigour to assure continuity of internet use and communication for all users.

### 2.3 English law

Clearly, all that we do must comply with English law, and our use of a network account is no exception. It therefore follows that, in addition to any ICTS-specific legal duty which is set out in appropriate specific legislation, 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 London network, and it is at all times the individual user's duty to be aware of what constitutes legal use and behaviour.

The Counter-terrorism and Security Act 2015 places duties upon the University, including monitoring, alerting and evidence-gathering procedures, to prevent the spread of terrorism and the drawing of people into terrorism. In addition to the countermeasures applied to electronic mail in general, these duties may involve investigation of the mail component of activity which is not *prima facie* ICTS-related.

---

<sup>2</sup> See <http://www.ja.net/documents/publications/policy/aup.pdf>

---

The Brunel Acceptable Computer Use Policy (BACUP) outlines duties related to this and other relevant legislative instruments.

## 2.4 Supranational jurisdictions

Over and above English law, we must always act within European and international law as we transact business using a network account.

## 2.5 Ethical soundness of practice

In all our work, there is the potential for mismatch between what is technically feasible and what is decent, respectful and just. Brunel University London's values encompass the highest standards of fairness, respect and decency in dealing with all people, and our use of data must be guided at all times by these values. When data are used in research, there is guidance, strengthened where necessary by regulation, through Brunel University London's policies for research ethics; the same guiding ethos must pervade all our work. It is the duty of each account-holder to act responsibly in furtherance of Brunel University London's values through ethically sound practice at all times: any lapse from the standards expected of a member of Brunel University London may result in the restriction or suspension of use of the account.

# 3 Components of network account management

It is useful to make sure that everyone is agreed on some definitions and forms of usage: here, we set out the use of certain terms in the context of Brunel University London network accounts.

## 3.1 Network account

A *Brunel University London network computer account* (within this Policy called an *account*) is the means by which a registered Brunel University London user may carry out business using computers connected to the Brunel University London data network for the creation, storage, analysis and management of data (not restricted to numeric data) using networked computers and like devices, or by which access is authenticated to facilities managed on behalf of the University by third parties, within the parameters set by the Brunel Acceptable Computer Use Policy (BACUP), by other relevant Policies, Rules and Regulations of Brunel University London, and by supervening laws. Indeed, this account is the only official means of conducting Brunel University London business electronically or with recourse to networked electronic devices, whereby these business data contribute to the official records of Brunel University London. It is therefore critically important that staff, students, and other account-holders use their Brunel University London network accounts for this business, and that regular and frequent management of these accounts is carried out to ensure compliance with all applicable rules, regulations, laws and policies.

Access is made to the account by the account-holder through password-protected login, using the network username provided by the Computer Centre and the password associated with that username. This password must be kept secure and in the user's (human) memory: any application to issue a replacement for a forgotten password must be made by the user in person, by visiting the Computer Centre Service Desk with her/his Brunel University London ID card as proof of identity, or by such equivalently authenticated electronic means as may be provided at certain times by the Computer Centre for the purpose.

## 3.2 Username

The Computer Centre will create the *username*<sup>3</sup> associated with the account in its standard structural format: this will be the primary key whereby the account-holder may gain access to the Brunel University London data network. This username will also function as the within-domain part of the account-holder's address for electronic mail (if the account has such a mail facility associated with it), so is not considered to be secret. Notwithstanding this lack of secrecy, each account-holder has a duty of care in avoiding unnecessary promulgation of Brunel University London usernames through inadequate security of action. In particular, these must not be divulged to a third party beyond Brunel University London except with the express permission of the Director of the Computer Centre. It is a vital element of our holding to Brunel University London's values that each user respects the potential will of others not to be identified unnecessarily to others who might seek to make undue and/or unsolicited contact for purposes unconnected with the primary academic or corporate business of Brunel University London.

## 3.3 Password

The Computer Centre will generate a *password* of an adequate level of complexity and security, and will issue this password to the account-holder as the account's secondary access key. This password must not be divulged to any other person, other than by express, explicit and documented permission of the Director of the Computer Centre or his agent duly authorised for the purpose, and the continuing security of access is the responsibility of the account-holder, through the maintenance of a secret password of an adequate level of complexity and security. If the security of the password is known or suspected to be compromised (actually or potentially), it is the duty of the user to inform the Computer Centre immediately. The Computer Centre, on learning from any reputable source of any such actual, suspected or potential compromise, may act (without the necessity of prior notification of the account-holder) to retrieve any diminution in security by revoking the password associated with any account, substituting another password of an adequate level of complexity and security, and may take any further steps deemed necessary to maintain the integrity of Brunel University London data.

---

<sup>3</sup> analogous terms in other institutions include 'usercode' and 'login ID': we prefer consistency of use of the term 'username'

Following any such action, the account-holder must attend the Computer Centre Service Desk before access may be resumed. The Computer Centre will not store a password *en clair*, in hardcopy or electronic form, beyond the initial issue to the account-holder: this means that a lost password cannot be re-issued, and that any succeeding access rights must be authenticated using a freshly generated password. Since the disclosure or unauthorised discovery of any password compromises the security of the entire Brunel University London data network, any transgression may lead to disciplinary proceedings appropriate to a serious breach of Brunel University London regulations.

### 3.4 Filestore

A standard network account will give access to networked filestore, some for the account-holder's own use ('home-directory' filestore), and some for managed shared use. If the account has a mail facility associated with it, filestore will be set aside for storage of mail and other messaging data. It is the account-holder's responsibility to manage all such filestore effectively and parsimoniously, and to ensure that, in each case, data storage is compliant with all relevant legislation and policies. It must be noted that, in the case of any facility managed on behalf of Brunel University London by a third party, storage may be located within or outwith the confines of the Brunel University London data network.

Networked filestore is managed by the Computer Centre (or by another agent of the University on behalf of the Computer Centre) according to agreed management and backup procedures. Backup copies of data are created for the sole purpose of system-wide disaster recovery: they must not be considered to be 'offline storage'.

In addition to networked filestore, the account-holder may have access to local filestore held on a workstation's hard disk(s), and there may be the facility to write to removable media (external hard drive, DVD, USB memory, etc.): as with networked filestore, the responsibility to comply with all relevant legislation, regulatory instruments and policies remains with the account-holder. Such local filestore is to be considered transient and inappropriate for the storage of any record of Brunel University London, since any refreshment of the operating system or malfunction of the disk risks irretrievable loss of data.

### 3.5 Primary purpose of network account

The reason for issuing a Brunel University London network account is to offer the account-holder access to facilities which further the academic or corporate business of Brunel University London. This is known as the *primary purpose* of the account.

Primary-purpose business must have priority at all times, and any other use may be deemed to lie outwith the terms of the granting of an account.

## 4 Entitlement to account

This section details the entitlement through the lifecycle of an account for each of the various classes of user. In most cases, the characteristics of entitlement are quite clear: in all cases, the Director of the Computer Centre has the authority to amend a particular characteristic of entitlement at his discretion.

Users should note that the Computer Centre will manage demographic data, contact details, etc.), relating to the account: it is the responsibility of the account-holder to inform the Computer Centre of any change in these data and of any change of status.

It should be noted by all that sanctions for transgression against the Brunel Acceptable Computer Use Policy, other relevant Policies or rules of Brunel University London, or any applicable legislation or regulatory instrument, may include the total or partial suspension of access by an account-holder and a subsequent review of the period and/or characteristics of access on any resumption of access privileges. The application of such a total or partial suspension of access overrides any presumption of access rights laid out in this Policy.

From time to time, the Computer Centre (or its duly appointed agent) may undertake maintenance, upgrading or administrative work on aspects of the network, and other bodies in the internet chain may likewise undertake such work: it is the responsibility of the account-holder to maintain awareness of such work schedules and of any risk of access diminution associated therewith. Brunel University London will not be held responsible for any loss or damage as a result of access diminution associated with such works.

In all cases outlined below, any manual procedure associated with the inauguration, change or demission of a network account may at certain times be replaced by an equivalent automated process as approved by the Director of the Computer Centre. Reference below to such manual procedures should be read to incorporate such automated equivalents.

### 4.1 Brunel University London's staff

A member of staff of Brunel University London will generally be issued with a network account for the duration of a contract of employment or an analogous agreement. The authority for conferring current Brunel University London staff status rests with the Director of Human Resources<sup>4</sup>. The continuing validity of each staff account will be reviewed on an annual basis by confirmation from the senior officer of the account-holder's unit of the University.

---

<sup>4</sup> or, as agreed, through a competent and duly appointed agent

---

### **4.1.1 Permanent**

As soon as possible after arrival at Brunel University London, a new permanent member of staff should attend (with the letter of contract or analogous credentials) the Computer Centre to be registered as an account-holder. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the dissolution (through resignation, retirement or other reason for termination) of the contract of employment or analogous agreement. There will be no right of access by the account-holder following such a termination. The Computer Centre shall accept advice on termination of a staff contract or analogous agreement from the Directorate of Human Resources.

### **4.1.2 Fixed-term**

As soon as possible after arrival at Brunel University London, a new member of staff with a fixed-term contract or analogous agreement should attend (with the letter of contract or analogous credentials) the Computer Centre to be registered as an account-holder. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the fixed term, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the contract of employment or analogous agreement. There will be no right of access by the account-holder following such a termination. It is the responsibility of the account-holder to inform the Computer Centre of any change to the term of contract by the presentation of the official letter of change: in particular, any extension to the termination date must be communicated in this way to the Computer Centre before the original termination date, otherwise all data pertaining to the account may be deleted from the Brunel University London data network on that date. The Computer Centre shall accept advice on termination of a staff contract or analogous agreement from the Directorate of Human Resources.

### **4.1.3 Temporary**

As soon as possible after arrival at Brunel University London, a new temporary member of staff should attend (with the letter of contract or analogous credentials) to the Computer Centre to be registered as an account-holder for an agreed period. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the agreed period, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the temporary contract of employment or analogous agreement. There will be no right of access by the account-holder following such a termination. It is the responsibility of the account-holder to inform the Computer Centre of any change to the term of contract by the presentation of the official letter of change: in particular, any extension to the termination date must be communicated in this way to the Computer Centre before the original termination date, otherwise all data pertaining to the account may be deleted from the Brunel University London data network on that date. The issue of an account to a temporary member of staff will require that the Senior Officer of the appropriate unit within the University accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. In general,

accounts for temporary members of staff are likely to have restrictions placed upon them to ensure Brunel University London's compliance with legislation and records management practice. The Computer Centre shall accept advice on termination of a staff contract or analogous agreement from the Directorate of Human Resources.

#### **4.1.4 Volunteer**

In the absence of a contract for paid employment, a volunteer (*i.e.*, unpaid) member of staff must furnish the Computer Centre, at the beginning of the period of working for Brunel University London, with appropriate credentials (including approval of the Senior Officer of the relevant unit of the University) in order to be registered as an account-holder for an agreed period. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the agreed period, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the volunteer's work agreement with Brunel University London. There will be no right of access by the account-holder following such a termination. It is the responsibility of the account-holder to inform the Computer Centre of any change to the term of agreement by the presentation of the official letter of change: in particular, any extension to the termination date must be communicated in this way to the Computer Centre before the original termination date, otherwise all data pertaining to the account may be deleted from the Brunel University London data network on that date. The issue of an account to a volunteer member of staff will require that the Senior Officer of the appropriate unit within the University accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. In general, accounts for volunteer members of staff are likely to have restrictions placed upon them to ensure Brunel University London's compliance with legislation and records management practice. It is the responsibility of the Senior Officer of any unit within the University to inform the Computer Centre of any change to the status of any volunteer working within that unit, or to the agreed period of access.

#### **4.1.5 Retired staff member**

On retirement from active Brunel University London service, the account held by a permanent member of staff will be closed. At the discretion of the Director of the Computer Centre, a member of staff who has retired following a long association with Brunel University London may be granted the use of a new account for the purpose of maintaining contact (principally by electronic mail) with Brunel University London. The status of a retired member of staff will preclude, due to widespread licensing restrictions, the use of much software licensed for Brunel University London's use.

#### **4.1.6 Non-retired former staff member**

Following departure from employment at Brunel University London, there is no entitlement to a network account for any person by virtue of status as a former member of staff of Brunel University London.

---

### **4.1.7 Field testing**

At the discretion of the Director of the Computer Centre, an account may be issued to a member of staff of Brunel University London for the purposes of field testing<sup>5</sup>. This account will be issued for a fixed period consistent with the requirement for field-testing the particular entity. At the end of this time period, there will be no access to the account, nor to its associated filestore.

### **4.1.8 Member of staff as a student**

If a member of staff is enrolled as a student of Brunel University London, then an account will be issued to that person in the capacity of a student on the appropriate course. These accounts will run concurrently while the person enjoys dual status. It is important, and is the responsibility of the account-holder, to ensure the separation of these two accounts, the staff account being used for activity related to the account-holder's employment, and the student account for course-related activity.

### **4.1.9 Support worker**

An amanuensis, note-taker or other support worker operating, by prior agreement with Brunel University London, *in loco studentis* will be considered to have account access as a delegate for the student concerned (see appropriate sections under *Brunel student*). Any account needed for administrative contact between the support worker *per se* and Brunel University London should be set up as an appropriate (probably temporary or fixed-term) staff account. The principal focus for such support workers will be Brunel University London's Disability and Dyslexia Service.

## **4.2 Brunel student**

A student duly registered on a course of study at Brunel University London will be entitled to an account tailored to the class of registration, for the duration of the course of study. In the majority of instances, the Computer Centre will use information made available in good time to Brunel University London by applicants to create accounts for expected registrands, these accounts to be enabled at the time of Brunel University London registration. However, the formal start of account creation begins following registration, and the enabling of a student account is contingent on appropriate Brunel University London registration. In any instance of a student's progression from one course of study at Brunel University London to another, there will be no entitlement of access during any gap between the termination of one course of study and registration at the start of the subsequent course of study, nor is there any general entitlement to the transfer of data between such accounts. The continuing validity of a student account is assured through the association of such accounts with relevant statuses within the student record system.

---

<sup>5</sup> for example, so that a lecturer may have a "student's-eye view" of learning materials under consideration or development

---

### **4.2.1 Pre-enrolment**

On registration for a prerequisite course prior to taking up a place on a course of study at Brunel University London, a student will, if the nature of the prerequisite course demands networked computer usage, become entitled to use an account associated with that course of study, for the duration of that course of study. Such an account will not normally be personal to the student, and there may well be restrictions placed upon its use in order that Brunel University London may comply with licensing restrictions. There will be no access to the account, nor to associated data, following the end of the prerequisite course.

### **4.2.2 Foundation**

On registration for a course of study leading to a foundation award at Brunel University London, a student becomes entitled to an account associated with that course of study, for the duration of that course of study. The standard point of issue for such an account will be during Brunel University London's process of Registration during the allotted time for the course cohort's attendance, on the production of the account-holder's currently-validated Brunel University London ID card (or an unvalidated Brunel University London ID card accompanied by officially-endorsed Registration papers), by the account-holder. After the closure of the Registration process, the point of issue for account details will be the Computer Centre Service Desk, and issue will proceed on production of the account-holder's currently-validated Brunel University London ID card. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end date of the course of study as indicated by the appropriate information within Brunel University London's Student Records system, or at an earlier point of dissolution caused by withdrawal from, or other discontinuation of, the course of study for whatever reason. There will be no right of access by the account-holder following such a termination. On any subsequent transfer to another course of study at Brunel University London, the student will receive a new account appropriate to that course of study. The Computer Centre shall accept advice on termination of a student's registration from the Head of Registry.

### **4.2.3 Undergraduate**

On registration for an undergraduate course of study at Brunel University London, a student becomes entitled to an account associated with that course of study, for the duration of that course of study. The standard point of issue for such an account will be during Brunel University London's process of Registration during the allotted time for the course cohort's attendance, on the production of the account-holder's currently-validated Brunel University London ID card (or an unvalidated Brunel University London ID card accompanied by officially-endorsed Registration papers), by the account-holder. After the closure of the Registration process, the point of issue for account details will be the Computer Centre Service Desk, and issue will proceed on production of the account-holder's currently-validated Brunel University London ID card. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end date of the course of study as indicated by the appropriate information within Brunel University London's Student Records system, or at an earlier point of

dissolution caused by withdrawal from, or other discontinuation of, the course of study for whatever reason. There will be no right of access by the account-holder following such a termination. On any subsequent transfer to another course of study at Brunel University London, the student will receive a new account appropriate to that course of study. The Computer Centre shall accept advice on termination of a student's registration from the Head of Registry.

#### **4.2.4 Taught postgraduate**

On registration for a postgraduate course of study by teaching at Brunel University London, a student becomes entitled to an account associated with that course of study, for the duration of that course of study. The standard point of issue for such an account will be during Brunel University London's process of Registration during the allotted time for the course cohort's attendance, on the production of the account-holder's currently-validated Brunel University London ID card (or an unvalidated Brunel University London ID card accompanied by officially-endorsed Registration papers), by the account-holder. After the closure of the Registration process, the point of issue for account details will be the Computer Centre Service Desk, and issue will proceed on production of the account-holder's currently-validated University ID card. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end date of the course of study as indicated by the appropriate information within Brunel University London's Student Records system, or at an earlier point of dissolution caused by withdrawal from, or other discontinuation of, the course of study for whatever reason. There will be no right of access by the account-holder following such a termination. On any subsequent transfer to another course of study at Brunel University London, the student will receive a new account appropriate to that course of study. The Computer Centre shall accept advice on termination of a student's registration from the Head of Registry.

#### **4.2.5 Research postgraduate**

On registration for a postgraduate course of study by research at Brunel University London, a student becomes entitled to an account associated with that course of study, for the duration of that course of study. After completion of Brunel University London's Registration process, account details will be issued to the account-holder at the Computer Centre Service Desk on production of the account-holder's currently-validated Brunel University London ID card. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end date of the course of study as indicated by the appropriate information within Brunel University London's Student Records system, or at an earlier point of dissolution caused by withdrawal from, or other discontinuation of, the course of study for whatever reason. There will be no right of access by the account-holder following such a termination. On any subsequent transfer to another course of study at Brunel University London, or otherwise to another status within Brunel University London, the student will receive a new account appropriate to the changed status. The Computer Centre shall accept advice on termination of a student's registration from the Head of Registry.

---

#### **4.2.6 Full-time student**

A full-time student will have account access rights in accordance with the Policies of Brunel University London during the period of registration for the course of study for which the account is issued, except during any period of suspension of access imposed for any reason as laid out in the Regulations and Policies of Brunel University London.

#### **4.2.7 Part-time student**

A part-time student will have account access rights in accordance with the Policies of Brunel University London during the period of registration for the course of study for which the account is issued, except during any period of suspension of access imposed for any reason as laid out in the Regulations and Policies of Brunel University London.

#### **4.2.8 Continuous professional development**

A student who undertakes modular study at Brunel University London within a programme of continuous professional development (or similar structure) is entitled to an account with characteristics appropriate to the learning outcomes of the module, for the duration of the module. Such an account may be non-personalised in character. After completion of Brunel University London's Registration process for the module, account details will be issued to the account-holder at the Computer Centre Service Desk on production of the account-holder's currently-validated Brunel University London ID card, or by an agreed agency. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end date of the module as indicated to the Computer Centre, or at an earlier point of dissolution caused by withdrawal from, or other discontinuation of, the module for whatever reason. There will be no right of access by the account-holder following such a termination.

On any subsequent enrolment on another module within the same or another course of study at Brunel University London, or otherwise to another status within the University, the student will receive a new account appropriate to the changed status. The Computer Centre shall accept advice on termination of a student's registration from the Head of Registry.

#### **4.2.9 Student on placement**

A Brunel University London student will have account access rights in accordance with the Policies of Brunel University London during any period of Work Placement as an integral part of the course of study for which the account is issued, except during any period of suspension of access imposed for any reason as laid out in the Regulations and Policies of Brunel University London. Rights of connection to the Brunel University London data network, or of access to data held therein or elsewhere, from a connection-point which is not owned or managed by Brunel University London<sup>6</sup>, is entirely at the

---

<sup>6</sup> for example, from the workplace during placement

---

discretion of the owner/manager of that connection point. See also *Student undertaking work for Brunel University London*.

#### **4.2.10 Former student**

There is no entitlement to an account at Brunel University London for any person by virtue of status as a former student of Brunel University London.

#### **4.2.11 Student undertaking work for Brunel University London**

If, during a course of study, a Brunel University London student undertakes work (whether or not for reward) for Brunel University London, an account will be issued with a status appropriate to the work being undertaken<sup>7</sup>, for the purpose of any computer use associated with that work. It is important, and is the responsibility of the student, to ensure that the separation of the two roles (as student and worker) is reflected in the separate use of the accounts as appropriate. It should be noted that this applies also to any period of work placement which is undertaken within the University by a Brunel University London student. See also the section(s) appropriate to the work role. Any application for an account under this heading must be accompanied by an endorsement from the member of staff of Brunel University London who is supervising the work: this member of staff will be the sponsor of the account, and will be responsible for the management of data associated with the account following the termination of the account at the end of the period of work.

#### **4.2.12 Distance learner**

A student enrolled upon a course of study by distance learning which is provided by Brunel University London is entitled to an account appropriate to the course of study. Distance learners are reminded that the Computer Centre reserves the right to take any measures necessary to authenticate any account-holder at the point of issue of account details and at any point thereafter, and to suspend access to any account at any time for reasons of suspected personation.

#### **4.2.13 Support worker**

If a student requires the services of an amanuensis, note-taker or other support worker (e.g., for reasons of disability), then the support worker may, by prior agreement with Brunel University London, gain delegate access *in loco studentis* to the student's account. The support worker's own business with Brunel University London should be carried out using an appropriate staff account (see appropriate sections under *Brunel University London's staff*).

---

<sup>7</sup> this will normally be as a Brunel member of staff

## 4.3 Union of Brunel Students

The Union of Brunel Students occupies a special place in the structure of network accounts: the Union is independent of the university, but its symbiotic status with respect to Brunel University London makes beneficial more general access rights than may be extended to other external bodies. Continuing validity of such account is assured by annual review and confirmation by the General Manager of the Union of Brunel Students.

### 4.3.1 *Student as elected officer*

Each of the elected offices has, at the discretion of the Director of the Computer Centre, an account for the transaction of the business of the office. These accounts remain in place from year to year, surviving the change in incumbent office-holders. Continuity is maintained through the co-sponsorship of these accounts by the General Manager of the Union of Brunel Students and the Human Resources Manager of the Union of Brunel Students. For reasons of compliance and records management, it is not appropriate for the officer to use this account for personal business.

If a student defers completion of a course of study at Brunel University London in order to take up sabbatical office in the Union of Brunel Students, the account for that course of study will remain available throughout the period of sabbatical office.

### 4.3.2 *Staff*

At the discretion of the Director of the Computer Centre, a member of staff of the Union of Brunel Students may be issued with an account to transact the business of the Union of Brunel Students in its relation to the business of Brunel University London. The characteristics of the account may differ from those of an account issued to an analogous member of staff of Brunel University London, for compliance and other reasons: there will be no access to the account after its termination.

### 4.3.3 *Student group account*

At the discretion of the Director of the Computer Centre, and following a petition by the President and General Manager of the Union of Brunel Students (as co-sponsors of the account), a group of students recognised as such by the Union of Brunel Students may be granted an account for the purposes of transacting the proper business of that group in its relations with the Union of Brunel Students and with Brunel University London. Such an account will have restrictions placed upon it for compliance and other reasons, and will normally lapse at the end of the academic year. There will be no access to the account following its termination. For reasons of compliance and records management, it is not appropriate for any member of the group to use this account for personal business or other business beyond the original scope: any infringement of the conditions of issue of such an account will normally lead to its immediate and summary termination.

---

#### **4.3.4 Staff group account**

At the discretion of the Director of the Computer Centre, and following a petition by the General Manager and Human Resources Manager of the Union of Brunel Students (as co-sponsors of the account), an account may be created for the purposes of transacting group-based business. For reasons of compliance and records management, it is not appropriate for any member of the group to use this account for personal business or other business beyond the original scope.

### **4.4 Trades unions at Brunel University London**

Brunel University London recognises certain trades unions as representative bodies for groups of staff within Brunel University London. Though these are third-party organisations (and therefore do not fall within much of the licensing structure of Brunel University London's software portfolio), there may be occasions when it is mutually beneficial to grant access to an account for agreed local business of one such trade union. In all cases, the granting of any account privileges will be strictly for specified purposes, will be at the discretion of the Director of the Computer Centre, and may be rescinded at any time at the sole discretion of Brunel University London.

The access privileges for such an account are likely to be severely restricted in comparison with those for a standard staff account, for reasons of contract, compliance and records management. Data stored upon, or passing through, the Brunel University London data network in connection with the use of such an account constitute records of the University, and must be managed as such. Responsibility for custody and content lies with the appropriate trade union: this, does not prevent Brunel University London from taking action (including disciplinary action) in the event of inappropriate usage of such an account. Continuing validity of such accounts will be assured by annual review, agreed by the senior officer of the appropriate Trade Union and the Director of Human Resources.

#### **4.4.1 Elected local officer**

At the discretion of the Director of the Computer Centre, a member of staff at Brunel University London, having been elected as an officer in a Brunel University London branch of a trade union duly recognised by Brunel University London, may be granted an account for the purpose of transacting specified business of the local branch on behalf of its members. Such an account will be issued for a fixed period, and there will be no rights of access to the account following its termination (whether at the end of the fixed period or following rescission at an earlier date). It is inappropriate for such an account to be used for purposes other than those agreed by the Director of the Computer Centre on behalf of Brunel University London, and any breach of this condition is likely to result in the immediate and summary termination of the account.

On any change of incumbency, the new officer must apply for the granting of account privileges in the manner laid out for a new account under this heading.

---

#### **4.4.2 Elected non-local officer**

There is no entitlement to an account for the transaction of business of a trade union duly recognised at Brunel University London where the duties associated with that office extend beyond activity carried out on behalf of its members employed by Brunel University London. Furthermore, it is inappropriate for any other Brunel University London account to be used for such purposes.

#### **4.4.3 Non-Brunel officers**

There is no entitlement to an account for the transaction of business of a trade union duly recognised at Brunel University London for anyone who is not a current member of staff of Brunel University London.

#### **4.4.4 Trades unions not recognised at Brunel University London**

There is no entitlement to an account for the transaction of business of a trade union not recognised as a representative union at Brunel University London.

### **4.5 Contractor**

From time to time, there is a requirement that a member of staff of an outside organisation should have access to the Brunel University London data network as an account-holder, in order to undertake specific tasks. The characteristics of such an account will vary according to the individual circumstances, and the exact terms and conditions will remain entirely at the discretion of the Director of the Computer Centre: the subsections of this part of the Policy indicate the principles under which such an account may be issued. Sponsorship of contractors' accounts may be devolved within the formal sponsor's hierarchy with the agreement of the Director of the Computer Centre.

Information and intelligence gained by a contractor through use of a Brunel University London account is privileged. Brunel University London reserves the right to seek appropriate redress (including legal proceedings where appropriate) following any abuse of such privilege.

Continuing validity of such accounts will be assured by review with a frequency commensurate with the characteristics of the contract, as described in the subsections below. In the absence of specific review schedules, the term will be annually on the anniversary of the granting of the account.

#### **4.5.1 Contract academic staff**

A member of staff from another academic institution may be contracted to undertake work for Brunel University London<sup>8</sup>: on request, an account may be created for computer use associated with such work. As soon as possible after the contract has been agreed, the account-holder should attend (with

---

<sup>8</sup> for example, to deliver course content as a visiting lecturer

the letter of contract or analogous credentials) the Computer Centre Service Desk to be registered as an account-holder for an agreed period. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the period agreed in the contract, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the contract. There will be no right of access by the account-holder following such a termination. The issue of such an account will require that the Senior Officer of the relevant unit of the University acts as sponsor of the account, thereby accepting responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. Continuing validity will be assured by annual confirmation by the relevant unit of the University: if at the time of such annual review, the contract has less than six months to run, the Senior Officer of the relevant unit of the University will be asked to confirm the end date or to authorise a new end date as appropriate.

In general, such an account is likely to have restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice.

The Computer Centre shall accept advice on termination of a staff contract or analogous agreement from the Directorate of Human Resources.

#### **4.5.2 *Outsourced services and facilities***

When a third-party organisation is contracted to provide outsourced services or facilities to Brunel University London in a manner which might be deemed analogous to an in-house provision, it may be beneficial that certain members of staff of that organisation should have an account on the Brunel University London data network for specific purposes of communication and collaboration with members of Brunel University London. The issue of such accounts will be at the discretion of the Director of the Computer Centre, and the business case must be made by the senior manager of the University charged with overseeing the outsourcing contract, that senior manager becoming the sponsor of the accounts.

On receipt of the application from the sponsor, the Computer Centre will, if the account is granted, process the registration as quickly as is practicable, subject to the operation of scheduled components of the registration process. The sponsor will be informed of the availability of the account, and the contractor may then be issued with the account details at the Computer Centre Service Desk.

The standard period of registration for any such individual account will be for the duration of the contract to supply such services/facilities (renewable in the case of an extension to the organisation's contract with Brunel University London, or in the case of a new contract's being agreed with the same organisation for continuing similar service), or at an earlier point of dissolution (through resignation, retirement, redeployment within the third-party organisation away from Brunel University London service, or other reason for termination) of the individual's contract with the third party, or the apart thereof which is aligned with work undertaken for Brunel University London). There will be no right of access by the account-holder following such a termination.

It is the responsibility of the third-party organisation to inform the Computer Centre (directly or via the sponsor as agreed) of any change in status of the account-holder in relation to that organisation. The issue of such an account will require that the sponsor accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. If, at the anniversary of the account's creation, the contract has less than six months to run, the Computer Centre will review the account's continuing validity with the sponsor.

In general, such an account is likely to have stringent restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice.

The Computer Centre shall accept advice on termination of a contract to supply outsourced services or facilities from the senior manager of the University charged with overseeing the contract. The Computer Centre shall accept advice on termination of an individual staff contract within the outsourced service from the Human Resources manager of the third-party organisation, or from a duly appointed on-site representative thereof.

### **4.5.3 Contractor company staff**

On occasion, it may be beneficial that a named member of staff of a company contracted to undertake work for Brunel University London should have an account on the Brunel University London data network for specific purposes of communication and collaboration with staff of the University. The issue of such an account will be at the discretion of the Director of the Computer Centre, and the business case must be made by the senior manager of the University charged with overseeing the contract with the outside company, that senior manager becoming the sponsor of the account. On receipt of the application from the sponsor, the Computer Centre will, if the account is granted, process the registration as quickly as is practicable, subject to the operation of scheduled components of the registration process. The sponsor will be informed of the availability of the account, and the contractor may then be issued with the account details at the Computer Centre Service Desk. The period of registration will be terminated at the end of the fixed period agreed in the contract, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the contract. There will be no right of access by the account-holder following such a termination. It is the responsibility of the contractor company to inform the Computer Centre (directly or via the sponsor as agreed) of any change in status of the account-holder in relation to the company. The issue of such an account will require that the sponsor accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. If, at the anniversary of the account's creation, the contract has less than six months to run, the Computer Centre will review the account's continuing validity with the sponsor.

In general, such an account is likely to have stringent restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice.

---

The Computer Centre shall accept advice on termination of a contract from the Directorate of Human Resources.

#### **4.5.4 *Supplier support staff***

On occasion, it may be beneficial that a named member of support staff of a supplier company should have an account on the Brunel University London data network for specific purposes of supporting Brunel University London's installation of equipment or services. The issue of such an account will be at the discretion of the Director of the Computer Centre, and the business case must be made by the senior manager of the University charged with overseeing the contract with the supplier company, that senior manager thereby becoming the sponsor of the account. On receipt of the application from the sponsor, the Computer Centre will, if the account is granted, process the registration as quickly as is practicable, subject to the operation of scheduled components of the registration process. The sponsor will be informed of the availability of the account, and the contractor may then be issued with the account details at the Computer Centre Service Desk. The period of registration will be terminated at the end of the fixed period agreed in the contract, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the contract. There will be no right of access by the account-holder following such a termination. It is the responsibility of the supplier company to inform the Computer Centre (directly or via the sponsor as agreed) of any change in status of the account-holder in relation to the company. If, at the anniversary of the account's creation, the contract has less than six months to run, the Computer Centre will review the account's continuing validity with the sponsor.

The issue of such an account will require that the sponsor accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. In general, such an account is likely to have stringent restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice; in certain cases, a waiver may need to be obtained from licensors before the account may be used.

The Computer Centre shall accept advice on termination of a staff contract or analogous agreement from the Directorate of Human Resources.

#### **4.5.5 *Field testing***

At the discretion of the Director of the Computer Centre, an account may be issued to a member of staff of a company under contract to Brunel University London for the purposes of field testing. This account will be issued for a fixed period consistent with the requirement for field-testing the particular entity. At the end of this time period, there will be no access to the account or to its associated filestore. In certain cases, a waiver may need to be obtained from licensors before the account may be used.

---

## 4.6 Lay member of Council

A lay member of the Council of Brunel University London is entitled to an account in order to facilitate Council business. Such an account will have the Secretary to the Council of Brunel University London as sponsor. On receipt of a request by the sponsor, the Computer Centre will process the registration as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the member's service on Council, or at an earlier point of dissolution on the instructions of the sponsor. There will be no right of access by the account-holder following such a termination. The assurance of continuing validity of such accounts will be met by annual review by the sponsor (or duly designated agent).

## 4.7 Associated persons

In addition to Brunel University London staff and students, several classes of person may be designated as 'associated' with Brunel University London. Sponsorship of associates' accounts may be devolved within the formal sponsor's hierarchy with the agreement of the Director of the Computer Centre. The assurance of continuing validity will be met by appropriate review as detailed hereunder.

### 4.7.1 *Professor Emeritus*

A Professor Emeritus of Brunel University London is entitled to an account for the purposes of maintaining academic communication with Brunel University London. The account will be issued by the Computer Centre for a fixed term (renewable) consistent with the likely period of activity, the characteristics of the account to be at the discretion of the Director of the Computer Centre. On receipt of the application from the Head of Registry (as sponsor), the Computer Centre will process the registration as quickly as is practicable, subject to the operation of scheduled components of the registration process, and will invite the Professor Emeritus to collect the account details. Assurance of continuing validity will be met by annual confirmation by the Head of Registry.

### 4.7.2 *Fellow of Brunel University London*

At the discretion of the Director of the Computer Centre, a person granted a Fellowship of Brunel University London may be issued with an account for the purposes of facilitating communication between the Fellow and Brunel University London. The account will be issued by the Computer Centre for a fixed term (renewable) consistent with the likely period of activity, the characteristics of the account to be at the discretion of the Director of the Computer Centre. On receipt of the application from the Head of Registry (as sponsor), the Computer Centre will process the registration as quickly as is practicable, subject to the operation of scheduled components of the registration process, and will invite the Fellow to collect the account details. Assurance of continuing validity will be met by annual confirmation by the Head of Registry.

---

### **4.7.3 Staff of associated institution**

At the discretion of the Director of the Computer Centre, a member of staff of an associated institution may be granted an account for purposes relevant to the association. The account will be issued by the Computer Centre for a fixed term (renewable) consistent with the likely period of activity, the characteristics of the account to be at the discretion of the Director of the Computer Centre. On receipt of the application from the prospective account-holder, the Computer Centre will process the registration as quickly as is practicable, subject to the operation of scheduled components of the registration process, and will invite the account-holder to collect the account details. The period of registration will be terminated at the end of the fixed term, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the status of the account-holder as a qualifying associate. There will be no right of access by the account-holder following such a termination. In the event of any misuse or compromise of such an account, the Director of the Computer Centre will have absolute discretion regarding the summary termination of the account, or of access thereto. Assurance of continuing validity will be met by annual confirmation by the account-holder.

### **4.7.4 Exchange student**

A student of another institution who is enrolled on a course of study within Brunel University London on an exchange basis as part of an award of the other institution is entitled to an account on the Brunel University London data network with characteristics appropriate to such status. The student should apply to the Computing Support Service Desk, with a currently-validated Brunel University London ID card as credentials. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end date of the course of study within Brunel University London, as indicated by the appropriate information within Brunel University London's Student Records system (the characteristics providing the necessary assurance of continuing validity), or at an earlier point of dissolution caused by withdrawal from, or other discontinuation of, the course of study for whatever reason. There will be no right of access by the account-holder following such a termination.

### **4.7.5 Student of associated institution – course award validated by Brunel University London**

A student of an associated institution who is enrolled on a course of study for an award which is validated by Brunel University London is entitled to an account on the Brunel University London data network with characteristics appropriate to such status. The student should apply to the Computing Support Service Desk, quoting the Brunel University London Student Number as entered in the Brunel University London Student Records system, and an identification from the associated institution, as credentials. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end date of the course of study as indicated by the appropriate information within Brunel University London's Student Records system (the characteristics providing the necessary assurance of continuing validity), or at an earlier point of dissolution caused by withdrawal from, or other discontinuation of, the

course of study for whatever reason. There will be no right of access by the account-holder following such a termination.

#### **4.7.6 *Student of associated institution – course award validated by student's home institution***

A student of an associated institution who is enrolled on a course of study for an award which is validated locally by that institution is not entitled to an account on the Brunel University London data network.

#### **4.7.7 *Academic collaborator***

Academic collaboration across institutional boundaries is well established, and in the vast majority of cases, operates across the boundaries of local institutional networks. In a few cases, however, it may be beneficial for a collaborator to use an account on the Brunel University London data network. The issue of such an account will be at the discretion of the Director of the Computer Centre, and will require the support of the senior officer of the appropriate unit within the University, who will be the sponsor of the account.

The collaborator should attend (with the letter of collaborative agreement or analogous credentials) the Computer Centre to be registered as an account-holder for an agreed period. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the period agreed in the collaborative agreement, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the collaborative agreement. There will be no right of access by the account-holder following such a termination.

The issue of such an account will require that the sponsor accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. Assurance of continuing validity will be by annual confirmation by the sponsor, and by a review with the sponsor at the final anniversary of the account's creation before the end date of the agreement. In general, such an account is likely to have restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice. In particular, access to licensed software may be limited.

Information and intelligence gained as a result of use of a Brunel University London network account is privileged. Legal restrictions on information sharing, put in place to ensure fair competition across the sector through consumer protection law, require that no relevant details of consumer choice (such as fee/scholarship structures) may be passed between institutions prior to their publication, and these considerations may restrict services available to account-holders of this category. It is the responsibility of the account-holder to behave proactively to avoid such intelligence leakage.

The Computer Centre shall accept advice on termination of a collaborative agreement from the Directorate of Human Resources.

---

### **4.7.8 *Non-academic collaborator***

Collaboration between staff of Brunel University London and non-academic partners is well established, and in the vast majority of cases, operates across the boundaries of local networks. In a few cases, however, it may be beneficial for a collaborator to use an account on the Brunel University London data network. The issue of such an account will be at the discretion of the Director of the Computer Centre, and will require the support of the senior officer of the appropriate unit within the University, who will be the sponsor of the account.

The collaborator should attend (with the letter of collaborative agreement or analogous credentials) the Computer Centre to be registered as an account-holder for an agreed period. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the period agreed in the collaborative agreement, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the collaborative agreement. There will be no right of access by the account-holder following such a termination.

The issue of such an account will require that the sponsor accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. Assurance of continuing validity will be by annual confirmation by the sponsor, and by a review with the sponsor at the final anniversary of the account's creation before the end date of the agreement. In general, such an account is likely to have stringent restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice. In particular, access to licensed software may be limited.

Information and intelligence gained as a result of use of a Brunel University London network account is privileged. Legal restrictions on information sharing, put in place to ensure fair competition across the sector through consumer protection law, require that no relevant details of consumer choice (such as fee/scholarship structures) may be passed between institutions prior to their publication, and these considerations may restrict services available to account-holders of this category. It is the responsibility of the account-holder to behave proactively to avoid such intelligence leakage.

The Computer Centre shall accept advice on termination of a collaborative agreement from the Directorate of Human Resources.

### **4.7.9 *Staff of associated company***

A member of staff of a company associated with Brunel University London (for example, a tenant company of the Science Park) may be granted an account on the Brunel University London data network in order to facilitate work undertaken there, particularly in respect of work undertaken in collaboration with Brunel University London. The commercial nature of the account-holder may necessitate restrictions of access and use, in order that Brunel University London might comply with regulatory and licensing conditions.

The granting of an account will be subject to four tests, *viz.*

- the discretionary approval of the Director of the Computer Centre
- the acceptance by JANET of any necessary petition (to be made by the Director of the Computer Centre) for access to and through the Joint Academic Network
- the successful agreement on appropriate cost recovery by the Computer Centre, and on any charges to JANET or other third parties
- the agreement of a fixed term (renewable) for the duration of the account

On the successful passing of the above tests, the Computer Centre will process the registration as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the agreed fixed period, or at an earlier point of dissolution (through resignation, retirement or other reason for termination) of the contract between the staff member and the associated company, or at the discretion of the Director of the Computer Centre. There will be no right of access by the account-holder following such a termination. It is the responsibility of the company to inform the Computer Centre (directly or via the University sponsor as agreed) of any change in status of the account-holder in relation to the company. Assurance of continuing validity will be by annual confirmation by the company or sponsor, and by a review with the company or sponsor at the final anniversary of the account's creation before the end date of the agreement.

The issue of such an account will require that the sponsor accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. In general, such an account is likely to have stringent restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice. In particular, access to licensed software may be limited.

## 4.8 Visitor

The ability of the University to accommodate visitors' requests for network access is severely limited by day-to-day pressures on its facilities, and by the need for Brunel University London and the account-holder alike to comply with all relevant legislative and licensing restrictions.

Sponsorship of visitors' accounts may be devolved within the formal sponsor's hierarchy with the agreement of the Director of the Computer Centre.

Information and intelligence gained as a result of use of such an account is privileged, and legal or regulatory restrictions may limit the services offered.

---

### **4.8.1 Visiting member of staff**

A member of staff of another academic institution who is visiting Brunel University London for an extended period may, at the discretion of the Director of the Computer Centre, be granted an account on the Brunel University London data network for an agreed fixed period. This will require the support of the senior officer of the appropriate unit within the University, who will be the sponsor of the account. The visitor should attend (with a letter of credence as to academic status) the Computer Centre to be registered as an account-holder for an agreed period. The registration will be processed as quickly as is practicable, subject to the operation of scheduled components of the registration process. The period of registration will be terminated at the end of the period agreed in the collaborative agreement, or at an earlier point of dissolution at the discretion of the Director of the Computer Centre. There will be no right of access by the account-holder following such a termination. Assurance of continuing validity will be met by annual confirmation by the sponsor, and by review with the sponsor on the last anniversary of the account's creation before the termination of the agreement.

The issue of such an account will require that the sponsor accepts responsibility for the user-level management of the account and all compliance issues, and for the management of any data associated with the account at the dissolution of the account-holder's access rights. In general, such an account is likely to have restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice. In particular, access to licensed software may be limited.

### **4.8.2 Conference delegate**

In general, a delegate attending a conference or similarly enjoying the benefits of Brunel University London (for example, a teacher, administrator or student at a summer school located at Brunel University London) has no entitlement to an account on the Brunel University London data network. An exception may be made, at the discretion of the Director of the Computer Centre, for members of the worldwide academic community attending an academic conference organised by a member of the academic staff of Brunel University London: for such people, non-personalised accounts may be created for the sole purpose of facilitating communication with the delegates' home institutions and/or full participation in the conference. In such an exceptional event, the business case must be made by the conference organiser to the Director of the Computer Centre at least three calendar months before the start of the conference. The conference organiser will be the sponsor of these accounts, and will bear all responsibility for ensuring that their use complies at all times with all relevant Policies of Brunel University London, and with all relevant legal and regulatory instruments. The termination date of these accounts will be an agreed date immediately following the end of the conference: there will be no entitlement of access other than during the conference and from locations previously agreed between the conference organiser and the Director of the Computer Centre.

In general, such an account is likely to have restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice. In particular, access to licensed software may be limited.

---

### **4.8.3 Student of another institution**

There is no general entitlement to an account on the Brunel University London Data Network for a student of another institution. *In extremis*, a petition may be made by the Head of the student's home department to the Director of the Computer Centre, outlining the case for the necessity of access using the Brunel University London data network.

The Director of the Computer Centre will have complete discretion on the granting or withholding of permission to enjoy the benefits of an account on the Brunel University London data network. Permission is unlikely to be granted if there is an alternative means whereby the student may communicate with the home institution. Assurance of continuing validity will be met by annual confirmation by the student,. In general, such an account is likely to have restrictions placed upon it to ensure Brunel University London's compliance with legislation and records management practice. In particular, access to licensed software may be limited.

## **4.9 Audit, review and quality assurance**

The functions of audit, of process review, and of quality assurance are well understood in maintaining academic and corporate standards, and in assuring taxpayers and other funders of Brunel University London of the appropriateness of our spending. The value placed by Brunel University London on transparency of process means that we are happy to facilitate such overview by the issue of appropriately provisioned accounts. It is likely that such accounts may enjoy more access privileges than a standard visitor account, so it is vital that each account-holder restricts the use of such privileges to the overview in hand. Assurance of continuing validity will be met by processes set out hereunder.

Information and intelligence gained as a result of use of a Brunel University London network account is privileged. Legal restrictions on information sharing, put in place to ensure fair competition across the sector through consumer protection law, require that no relevant details of consumer choice (such as fee/scholarship structures) may be passed between institutions prior to their publication, and these considerations may restrict services available to account-holders of this category. It is the responsibility of the account-holder to behave proactively to avoid such intelligence leakage.

We acknowledge the benefits of considered dissemination of good practice, and the key role that such activity plays in review processes; however, there may be occasions, at the discretion of the Director of the Computer Centre in consultation with relevant senior management within Brunel University London and its professional counsel, when restrictions are placed on access.

### **4.9.1 Audit**

As part of the standard function of audit (whether financial audit, internal audit, an audit of regulatory compliance, or similar undertaking) of any part of Brunel University London, it may be necessary for external persons to gain access to the Brunel University London data network in various capacities, including the acting out of actions of a typical member of a particular class of user, or of several such. The Director of the Computer Centre and the Head of IT Governance will co-operate with the

---

investigative body concerned to optimise the provision of appropriate access, and will agree terms and conditions for account management.

If there is an ongoing contract for audit with a third party, standing (generic) accounts may be created to be re-issued (with fresh passwords) to successive auditors from that third party. According to best practice, stored data will be flushed from the account before re-use by an incoming auditor, or by the same auditor for a different audit diet. Such an account will normally be issued with termination *sine die*, or to coincide with the termination of the contract to provide audit services (as for other outsourced services). Assurance of continuing validity will be met by annual confirmation by the Head of IT Governance.

In the absence of an ongoing contract, an audit account will be set up for a fixed period at the discretion of the Director of the Computer Centre and/or the Head of IT Governance. In the case of the absence of the Director of the Computer Centre, or in the case of a possible conflict of interest, terms and conditions regarding audit account management may fall, as appropriate, to the Head of IT Governance, or to the Secretary to the Council of Brunel University London.

#### **4.9.2 Programme review**

Reviews of academic programmes may require that external reviewers may gain access to the Brunel University London data network in various capacities, including the acting out of actions of a typical member of a particular class of user, or of several such. The Director of the Computer Centre and the Head of IT Governance will co-operate with the review body concerned to optimise the provision of appropriate access, and will agree terms and conditions for account management accordingly, in consultation with the Senior Officer of the University charged with overseeing academic quality and standards. If the terms of the review are ongoing and 'impersonal', standing (generic) accounts may be created to be re-issued (with fresh passwords) to successive reviewers. According to best practice, stored data will be flushed from the account before re-use by an incoming reviewer, or by the same reviewer for a different review. Such an account will normally be issued with termination *sine die*.

In the absence of an ongoing review, a reviewer's account will be set up for a fixed period at the discretion of the Director of the Computer Centre.

Assurance of continuing validity will be met by annual confirmation by the Head of IT Governance.

#### **4.9.3 Professional accreditation**

The accreditative requirements of certain courses with competent professional regulatory bodies may require access for the accreditor(s). Access will be granted in line with academic programme review (above), but there may be restrictions placed upon the use of the account consistent with accreditor status. Assurance of continuing validity will be met by annual confirmation by the Head of IT Governance.

---

#### **4.9.4 External examiner and analogous status**

External examiners may, as part of their duties, need to gain access to the Brunel University London data network in various capacities, including the acting out of actions of a typical member of a particular class of user, or of several such, and to maintain oversight of processes and documentation. In most cases, the external examiner must be able to work analogously with staff members in the unit under advisement, a little more closely than an academic visitor, and the characteristics of an external examiner's account management will reflect this status.

The Director of the Computer Centre and the Head of IT Governance will co-operate with the Senior Officer of the University charged with overseeing academic quality and standards associated with the discipline under advisement, and with the Senior Officer of any relevant academic unit of the University, to optimise the provision of appropriate access, and will agree terms and conditions for account management accordingly, in consultation with these office-holders.

An external examiner's account will be issued for the duration of the agreement to act in that capacity. If an external examiner's term of duty is extended, or if he/she is re-appointed for a contiguous successive term, the account's termination date will be adjusted accordingly. On termination of the account, discussions will take place with the senior officer of the University charged with overseeing academic quality and standards (independent of academic subject), to ensure the orderly transfer of appropriate files for retention under Brunel University London's Document Management policies; only after sign-off from this procedure will the account be removed and the data held in that account obliterated. Assurance of continuing validity will be met by annual confirmation by the Head of Registry or the Head of IT Governance.

#### **4.9.5 Academic quality assurance**

The assurance of academic quality is, in essence, an audit, and account provision will follow the practice outlined for the audit function, with the additional proviso that the Director of the Computer Centre and the Head of IT Governance will work with the Senior Officer of the University charged with overseeing academic quality and standards in deciding upon the terms and conditions of issue of an account for the purpose of academic quality assurance. Assurance of continuing validity will be met by annual confirmation by the Head of IT Governance.

#### **4.9.6 Analogous function**

The grant of an account for an analogous function will be wholly at the discretion of the Director of the Computer Centre, with the Secretary to the Council of Brunel University London and the Head of IT Governance to deputise in the case of the absence of the Director, or in cases of recusation due to a possible conflict of interest: terms and conditions for similar functions will inform decisions. Assurance of continuing validity will be met by annual confirmation by the Head of Registry or the Head of IT Governance.

---

## 4.10 External account-holder

The final category of prospective account-holder is, naturally, the most nebulous — the ‘external person’.

### 4.10.1 *General external account-holder*

In general, there is no entitlement of account for a general external person. However, the Director of the Computer Centre has the authority to grant account access at his discretion, and to attach terms and conditions upon any account so granted. Assurance of continuing validity will be met by annual confirmation by the Head of Registry or the Head of IT Governance.

## 5 Acceptable categories of use

Brunel University London provides ICTS<sup>9</sup> facilities (including network accounts) for use in the furtherance of the learning, teaching, research and approved business activities of Brunel University London: activity which conforms to the above is defined as ‘primary-purpose use’.

Brunel University London’s facilities, including such facilities as are provided by Brunel University London but managed on behalf of Brunel University London by a third party, should not be used for

- personal use at a level which has the potential to impinge on primary-purpose use of Brunel University London facilities.
- the use or storage of unsolicited commercial, advertising or petitioning material (including any such mail in conjunction with any individual, not-for-profit, political, religious, advocative or charitable entity as well as a commercial third party).
- the unauthorised use by a third party of confidential material concerning the activities of Brunel University London.
- any information sharing which may contravene the letter or spirit of consumer protection law as it applies to the assurance of fair competition and fair access across the Higher Education sector in the United Kingdom, the European Union, and elsewhere as relevant.
- the use of material which infringes the intellectual property rights (including, but not confined to, copyright and patent protection) of another person or other legal entity.
- the creation, transmission, use and/or storage of any offensive, obscene or indecent images, data or other material unless by an individual registered as having a research or work-related requirement to interact with such material.

---

<sup>9</sup> Information and Communications Technology and Services

- 
- the use of any network account to promote activity which is the subject of restriction under the Counter-terrorism and Security Act 2015, or to make a connection to an external site in order to promote such activity
  - any activity likely to harm the reputation of Brunel University London or the goodwill extended to Brunel University London.

In all cases and at all times, the account-holder is bound by the Brunel Acceptable Computer Use Policy<sup>10</sup> while using the facilities offered by or through the Brunel University London data network.

## 6 Ownership, custody, agency and disclosure

These aspects of management of information by account-holders touch upon key aspects of behaviour. It is important to bear in mind at all times the legal, regulatory and moral principles which apply.

Of these, the last is perhaps the most difficult to pin down and the easiest to break. The rule must be to afford the greatest respect to the subjects of our information, while not impeding the free flow of Brunel University London business unnecessarily: such respect covers the broadest collection of topics, from the care of data in transit to unceasing vigilance in ensuring that correct names and other demographic details are used at all times.

### 6.1 Ownership

All data created and maintained on computer systems within the Brunel University London data network become the sole property of Brunel University London, unless there is an explicit arrangement to the contrary agreed by the University. Brunel University London deploys countermeasures against the infiltration of its systems by viruses, worms and other vexatious items, and data which are deemed to exhibit high probabilities of being vexatious may be quarantined, deleted or otherwise managed in order to minimise the risk of disruption to the work of Brunel University London or of financial loss to Brunel University London, or to maintain the reputation of Brunel University London.

Brunel University London will not be held responsible for any loss or injury caused by the actions of such countermeasures, or through any downstream consequences of such countermeasures' being applied in the pursuance of due purpose.

---

<sup>10</sup> available at <http://www.brunel.ac.uk/life/study/computer-centre/policies/>

---

## 6.2 Official record of Brunel University London

Data which contribute to the academic or corporate business of Brunel University London become part of the corpus of official records of Brunel University London. For this reason, such business must be transacted using the official account(s) provided by Brunel University London for the purpose.

The data, once created, edited or otherwise used, become subject to Brunel University London records management policies and will, where relevant, become available for lawful disclosure to third parties (for example, under Freedom of Information legislation).

It is the responsibility of any person holding multiple accounts to ensure that each piece of business is transacted using the account issued for such business in accordance with all relevant policies of Brunel University London. Responsibility for Brunel University London's policies in records management lies within the Governance, Information and Legal Office of Brunel University London.

## 6.3 Personal use of the account

Brunel University London encourages the use of appropriate information technology, and allows a network account to be used for personal purposes *in extremis* as long as the use

- is reasonable, is not disproportionate to primary-purpose use, nor is in any way detrimental to the system's full availability for primary-purpose use.
- is not for commercial or profit-seeking purpose, nor in furtherance of any financial gain to the sender or (by the agency of the sender's solicitation) to any third party, nor in furtherance of the dissemination of the aims, ethos, policies, opinions or like matter in respect of any third party, including, it should be noted, any individual, not-for-profit, political, religious, advocative or charitable entity as well as a commercial third party.
- does not promote activity which is the subject of restriction under the Counter-terrorism and Security Act 2015, whether by direct use of the account or by making a connection to an external site in order to promote such activity.
- does not conflict with the rules, regulations, policies and procedures of Brunel University London.
- is not of a nature that conflicts with the business of Brunel University London.
- is not of a nature which could lead to a diminution of Brunel University London's reputational integrity.

and as long as there is no feasible alternative (for example, cloud-computing access to personal file storage and applications) to use of the Brunel University London account.

## 6.4 Monitoring data

Brunel University London has a right to inspect, monitor or disclose data stored upon or passing through the Brunel University London data network, but will not, as a matter of routine, do so unless

- required by law (including the duties placed upon the University to undertake risk-based monitoring, alerting and evidence-gathering under legislation such as, but not limited to, the Counter-terrorism and Security Act 2015).
- for the purposes of maintaining the free flow of primary-purpose business of Brunel University London.
- as part of an investigation of a suspected violation of the ordinances, rules, regulations or policies of Brunel University London.

Brunel University London's policies on the inspection, monitoring and disclosure of data are founded upon compliance with all relevant legislation, and with the Seven Principles of Public Life (popularly known as the Nolan Principles)<sup>11</sup>, and with the University's values of fairness, respect and decency.

## 6.5 Custody of data

Responsibility for safe and secure custody of data stored within the Brunel University London data network lies with the file owner<sup>12</sup>: it is the file owner's responsibility to ensure that any person with access to the data is conversant with the responsibilities of a data user, and abides by any compliance requirements.

## 6.6 Custody by agency

The appointment of an agent (or of several agents working individually or collectively) with partial or total access privileges to data stored by the account-holder does not change the responsibility for any action. The account-holder remains responsible for all data stored within any filestore associated with the account<sup>13</sup>, and the agent who creates, edits, deletes or otherwise acts upon the account-holder's data is responsible for compliance with all relevant Policies and rules of Brunel University London, and with all relevant supervening policies, rules and legislation, in the carrying out of any such action.

## 6.7 Disclosure

Data may be disclosed to a third party under circumstances which are germane to the proper operation of the academic and corporate functions of Brunel University London. Advice will be sought from the

---

<sup>11</sup> See, for example, <http://www.archive.official-documents.co.uk/document/parlment/nolan/nolan.htm>

<sup>12</sup> file ownership is independent of the ownership of data

<sup>13</sup> including such storage locations as shared-access repositories in SharePoint or similar applications

Governance, Information and Legal Office of Brunel University London whenever there is any doubt about the legitimacy of disclosure. In support of the lines of authority for disclosure as laid down below, the Chief Operating Officer and the Vice-Principals have authority to act in the absence of primary authorities, as do, *in extremis*, the Director of the Computer Centre and Secretary to Council.

In addition, normal operation of the Brunel University London data network may, in the context of a technical investigation, result in “accidental disclosure” within the investigative team: see also the subsections below on technical investigation (within sections discussing delegated access). Note also the section on *Professional immunity* below.

In addition, it should be noted that disclosure under certain legislation, such as the Counter-terrorism and Security Act 2015, will be undertaken with due regard to balancing legislation — see the section of the Brunel Acceptable Computer Use Policy (BACUP) which refers to this Act.

### **6.7.1 Disclosure of business data**

First and foremost, it should be noted that all data held within a Brunel University London network account are deemed to be ‘business data’ of Brunel University London. Data which are clearly labelled as personal, and which are stored accordingly and adequately separately from other data, will be observed as such in manual transactions, though automated data transactions will generally be unable to distinguish between the two types of designation. This highlights the clear benefits of rigorous separation of personal and business data, preferably to the extent of using an external account for all activity which is not Brunel University London business. Authority for the release of business data to be disclosed to a third party is vested initially in the normal line management of Brunel University London, and alternatively (and directly in the case of disclosure from a student account) in the Senior Officer of the relevant unit of the University.

### **6.7.2 Disclosure of data identified as personal**

The identification of data as personal does not *per se* invalidate rights of disclosure within the meaning of Data Protection and Freedom of Information legislation. Users are reminded that inadequate identification or storage management will cause the data to be treated immediately as business data.

Authority for the release of data adequately identified as personal will rest with

- the Senior Officer of the relevant academic unit of the University, in the case of disclosure from a Brunel University London student account (*i.e.*, one classified within the subsections of accounts under *Brunel student* above).
- the Director of Human Resources, in the case of disclosure from any account other than a Brunel University London student account (as defined above).

## 7 Principles of access

It is important to separate out the two strands of the principles of access when dealing with a Brunel University London network account: these are

- access to a Brunel University London network account by the account-holder and others.
- access to data within a Brunel University London network account by the account-holder and others.

These are covered in subsections below. It is important to realise that access permission may not be controlled exclusively by technical means — indeed, it may not be controllable by technical means — and the power of a verbal or written contract of instruction is not lessened by the existence (or otherwise) of technical controls. Likewise, the absence of any relevant technical control does not lessen the need for legal and moral vigilance.

Information and intelligence gained as a result of use of a Brunel University London network account is privileged. Legal restrictions on information sharing, put in place to ensure fair competition across the sector through consumer protection law, require that no relevant details of consumer choice (such as fee/scholarship structures) may be passed between institutions prior to their publication, and these considerations may restrict services available to account-holders of this category. In like manner, there may be legal and regulatory constraints which govern specifics of access pertaining to individual use profiles.

It is the responsibility of the account-holder to behave proactively to avoid such intelligence leakage.

### 7.1 Access to a network account

An account-holder's primary mode of access to a Brunel University London network account will be via a workstation which is connected to the Brunel University London data network, either in a public-domain workarea or (with the permission of the primary user of the workstation) in an office or similar environment. In this manner, the traffic transacted between the account-holder and the Brunel University London data network lies wholly within the University. Access may be made to a network account from another location if the University is satisfied that an appropriate level of security is provided in making and using the connection. The Director of the Computer Centre has the discretion to allow or disallow access from any location or class of locations, or from the use of any mode or class of modes, and to change such designation at any time, for any purpose related to the free flow of primary-purpose Brunel University London business or to the integrity of Brunel University London data or its services.

It is the responsibility of the account-holder to ensure that all aspects of this policy and of any other relevant legislation and regulations are observed in any access to a Brunel University London network

account. Access to a network account by a person other than the account-holder may only be made with the express sanction of the Director of the Computer Centre or his nominated representative.

## 7.2 Access to data within a network account

Once access has been gained to a Brunel University London network account, an account-holder has access to such data within the account as may be served to the point of access — users should note that there may be certain limitations on access from beyond Brunel University London, or through the use of a mode of access other than that recommended as primary access-mode for the account.

Access to data owned by another Brunel University London account-holder may be granted (within the provisions of all relevant policies, regulations and legislation) for primary-mode access: there may be restrictions on access to such data if account access had been gained by another means or from beyond Brunel University London.

The Director of the Computer Centre has the discretion to allow or disallow access to any data from any location or class of locations, or from the use of any mode or class of modes, and to change such designation at any time, for any purpose related to the free flow of primary-purpose Brunel University London business or to the integrity of Brunel University London data or computing services.

It is the responsibility of the accessor to ensure that all aspects of this policy and of any other relevant legislation and regulations are observed in any access to Brunel University London data, and of the owner of the data to ensure that each permitted accessor is aware of the responsibilities associated with the granting of access and with the possibility of access restriction. It is furthermore the duty of the accessor to access and use information only in accordance with the University's values of decency, respect and fairness.

## 8 Delegation of access by the account-holder

Under certain conditions, full or partial access to data held in filestore may be delegated by the account-holder to the holder of another account on the Brunel University London data network. By such an action, the account-holder does not relinquish any responsibility with respect to the operation of the account. The agent also bears responsibility for compliance with all relevant policies, rules and legislation in carrying out any action on the delegator's account.

The delegation of any access is a serious matter, and must be carried out in accordance with the rules and policies drawn up by Brunel University London, by JANET, and by other relevant parties. All users should note particularly that it is forbidden to disclose any password which might allow another person to gain access in a manner which could lead to personation of the account-holder. The account-holder should maintain records which detail the timings and scope of any such delegation, whether a new delegation, a change to an existing delegation, or the withdrawal of delegate access.

It is important to realise that delegated access permission may not be controlled exclusively by technical means — indeed, it may not be controllable by technical means — and the place of a verbal or written contract of instruction is not lessened by the existence (or otherwise) of technical controls. Likewise, the absence of any relevant technical control does not lessen the need for legal vigilance on the part of either the delegate or the delegator in any delegative agreement.

It is furthermore the duty of anyone granting delegate access to ensure the delegate's compliance with Brunel University London's standards and values of fairness, respect and decency in all use of information.

In each instance, every attempt must be made to secure appropriate access to the data associated with the account without in any way compromising the account-holder's access by changing the access password or any similar means.

## 8.1 Agent

Perhaps the most well-known instance of delegation within a Brunel University London network account is the granting of full or partial access privileges to a secretary or similar: in this instance, the delegate is acting as an agent for the principal. The scope of delegation should be clearly laid out in a message to the delegate, and this message should be retained and managed according to the standard procedures for task-related direction — any subsequent change to this delegation should be similarly managed. This procedure is important in maintaining an ability to confirm the delegated powers in any dispute or investigation.

## 8.2 Deputy

There will be times when a principal will give delegate authority to a deputy during a period of the principal's absence. This will often be rolled in with other delegate powers (for example, to act and take certain decisions on behalf of the principal).

The scope and duration of delegation should be clearly laid out in a message to the delegate, and this message should be retained and managed according to the standard procedures for task-related direction — any subsequent change to this delegation should be similarly managed. This procedure is important in maintaining an ability to confirm the delegated powers in any dispute or investigation.

## 8.3 Group member

There are many instances within Brunel University London of data simultaneously made available to all members of a peer group<sup>14</sup>. In the management of such data, the group members must always ensure that they act on behalf of the group. Each member of the group bears the responsibility to

---

<sup>14</sup> such as **computing-support**

---

maintain group records, but the line manager or other duly appointed head of the group bears ultimate responsibility for the management of all group records.

The scope and duration of delegation should be clearly laid out in a message to each group member, and this message should be retained and managed according to the standard procedures for task-related direction — any subsequent change to this delegation should be similarly managed. On any change to group membership, a fresh statement of delegation (superseding all previous statements) will be sent to each group member. This procedure is important in maintaining an ability to confirm the delegated powers in any dispute or investigation.

## 8.4 Stand-in

On occasion, there may be a need to grant access to a stand-in, possibly in an emergency. It is always helpful if the principal is able to make the delegation, but with the agreement of the Senior Officer of the principal's unit of the University the details of delegation may be conveyed to the Computer Centre (via Computing Support in the first instance) if direct delegation is not possible. The scope and duration of delegation should be clearly laid out in a message to the delegate (and, in the case of Computer Centre action, to the principal and to the Senior Officer of the principal's unit of the University), and this message should be retained and managed according to the standard procedures for task-related direction — any subsequent change to this delegation should be similarly managed. This procedure is important in maintaining an ability to confirm the delegated powers in any dispute or investigation.

Approval of the Director of Human Resources will be necessary before any application made by a third party will be considered.

In support of these lines of authority, the Chief Operating Officer and the Vice-Principals have authority to act in the absence of primary authorities, as do, *in extremis*, the Director of the Computer Centre and Secretary to the Council of Brunel University London.

## 8.5 Technical investigation

A Brunel University London user may, through a service enquiry, request a technical investigation which must necessarily result in access to that user's data by a third party: this will be considered delegate access with the consent of the account-holder.

### 8.5.1 Authorities

Authority for amending or halting a technical investigation which has been requested by an account-holder may be given by any one of the following investigative authorities, *viz.*

- the Vice-Chancellor
- the Chief Operating Officer
- the Director of Human Resources

- the Director of the Computer Centre

The boundaries for such access will be set (and may be changed) in respect of each individual investigator and for each individual investigation by any one of the above investigative authorities, who must make any relevant declaration of interest before proceeding.

### **8.5.2 Accidental disclosure**

During the course of a technical investigation into the Brunel University London network service, there may occur the need for data to be processed in such a way that the content is disclosed within the investigative team. Notwithstanding the consent given by the user to allow delegate access, such accidental disclosure places grave responsibilities upon each and every member of the investigative team.

Each such investigation is different, but the following rules apply in each case.

- The use of accidental disclosure must be limited to the minimum level consistent with the investigative procedure.
- Any information gained by accidental disclosure is privileged information, and the use of such information must be limited to the investigative procedure.
- Further disclosure to any other person within the investigative team beyond the minimal scope necessary to the investigation is not permitted.
- The technical capability of an investigative tool to facilitate accidental disclosure does not give the investigator automatic rights to use that tool to effect an accidental disclosure.

Any of the investigative authorities may place further restrictions on any individual investigator with respect to accidental disclosure, either in a particular investigation or generally. Any investigator who operates beyond the scope of the in-force rules with respect to accidental disclosure will be subject to the appropriate disciplinary procedures of Brunel University London.

## **9 Access beyond the account-holder's delegation**

There will be times when it is impossible to have the account-holder give express authority to grant partial or total access to the account. In this case, the Computer Centre must act in conjunction with the relevant senior managers of Brunel University London<sup>15</sup> and with the Senior Officers of relevant units of the University. In all cases, it is the duty of anyone granting delegate access to ensure the

---

<sup>15</sup> usually the Director of Human Resources in the case of a staff account, or the Head of Registry in the case of a student account: both may be involved in the case of staff access to a student account

delegate's compliance with Brunel University London's standards and values of fairness, respect and decency in all use of information.

## 9.1 Business or academic continuity

If the academic or business continuity of Brunel University London is put at risk by the inability of an account-holder to manage an account or data therein, the Senior Officer of the account-holder's unit of the University may request that delegate powers be assigned as if the account-holder has made such an assignment. This request should be made to the Assistant Director (User Services), detailing the scope and duration of the delegation. In making such a delegation, the senior officer of the relevant unit of the University will take responsibility for the good conduct of the delegate(s), and for the eventual management of the records created, edited or deleted on the delegated account. The Director of Human Resources may act for and on behalf of the Senior Officer of any unit of the University.

## 9.2 External lawful authorities

The Director of the Computer Centre will co-operate with any investigation by external lawful authorities, granting such access as is backed up by the appropriate Production Order, warrant or similar document, within the provisions of the appropriate legislation.

Any information gained by any member of an investigative team is privileged.

## 9.3 Internal disciplinary process

Data held within the Brunel University London data network which may be of evidential value in the pursuit of an internal disciplinary process may be disclosed appropriately as part of that process: this may require access beyond the account-holder's delegation. In addition to the involvement of those persons involved with the disciplinary process *per se*, there may be a requirement for technical investigators to become involved, and thus for access and accidental disclosure within the terms of such a technical investigation (*qv*).

### 9.3.1 Staff

The principal authority for access in relation to a staff disciplinary process will be the Director of Human Resources.

### 9.3.2 Student (academic discipline)

The principal authority for access in relation to an academically-related student disciplinary process will be the Head of Registry.

---

### **9.3.3 Student (non-academic discipline)**

The principal authority for access in relation to a non-academically-related student disciplinary process will be the Chief Operating Officer.

## **9.4 Technical investigation**

In the course of normal working, there must be access to entities within any system for the purposes of technical investigation. In the case of network accounts, this may involve competent technical staff of Brunel University London and its agents to require access without explicit delegation by the account-holder.

### **9.4.1 Authorities**

Authority for initiating or halting such a technical investigation may be given by any one of the following investigative authorities, *viz.*

- the Vice-Chancellor
- the Chief Operating Officer
- the Director of Human Resources
- the Director of the Computer Centre

In addition, day-to-day investigatory operations may involve such access in the undertaking of particular tasks (for example, in managing countermeasures against vexatious matter).

The boundaries for such access will be set (and may be changed) in respect of each individual investigator by any one of the above investigative authorities who must make any relevant declaration of interest before proceeding.

### **9.4.2 Accidental disclosure**

During the course of a technical investigation into the service, there may occur the need for data to be processed in such a way that content is disclosed within the investigative team. Such accidental disclosure places grave responsibilities upon each and every member of the investigative team.

Each such investigation is different, but the following rules apply in each case.

- The use of accidental disclosure must be limited to the minimum level consistent with the investigative procedure.
- Any information gained by accidental disclosure is privileged information, and the use of such information must be limited to the investigative procedure.
- Further disclosure to any other person within the investigative team beyond the minimal scope necessary to the investigation is not permitted.

- Disclosure to any person outwith the investigative team is not permitted, save with the prior, explicit and written authority of the Vice-Chancellor, Chief Operating Officer, Director of Human Resources, or the Director of the Computer Centre, countersigned wherever feasible by a second member of that quartet.
- The technical capability of an investigative tool to facilitate accidental disclosure does not give the investigator automatic rights to use that tool to effect an accidental disclosure.

Any investigative authoriser may place further restrictions on any individual investigator with respect to accidental disclosure, either in a particular investigation or more generally.

Any investigator who operates beyond the scope of the in-force rules regarding accidental disclosure will be subject to the appropriate disciplinary procedures of Brunel University London.

## 9.5 Technical operations

In the course of normal working, there must be access to entities within any system for the purposes of technical operation. In the case of network accounts, the need to maintain the smooth operation of dataflow and allied services, and to plan and execute enhancements thereto, may involve competent technical staff of Brunel University London and its agents to require access without explicit delegation by the account-holder. Furthermore, simple good practice for the purposes of business continuity will require that access permissions are held by competent technical staff.

Such access, which will only be invoked in emergency or through technical necessity, is privileged and the inappropriate disclosure or use of information gained through such accidental access will be handled through normal disciplinary channels and procedures.

See also *Professional immunity* below.

## 10 Management and filtering

In order to maintain continuity of Brunel University London's academic and corporate business, and in the safeguarding of Brunel University London's reputational integrity, Brunel University London will impose such management and filtering of data as it sees fit. Great care will be taken in such management to avoid the inadvertent loss of genuine data which advance the business of Brunel University London, but it is recognised that automatic filtering, however efficient, remains an inexact science.

---

## 10.1 Countermeasures against vexatious matter

Brunel University London will deploy countermeasures against the attempted infiltration of the Brunel University London data network by vexatious matter from whatever source or apparent source. In respect of facilities provided by Brunel University London but managed on behalf of Brunel University London by a third party, the relevant third party may apply its own countermeasures for like purpose. Brunel University London cannot be held responsible for any loss or damage consequent upon the reasonable application of such countermeasures.

At the discretion of the Computer Centre, the automated management may incorporate a notification (in real time or according to a notification schedule) to an intended recipient of any quarantining or deletion of data.

## 10.2 HTML filtering

Brunel University London deploys countermeasures against vexatious and offensive Web content. For this reason, filtering and management may be applied to HTML-based data and Web usage in areas including (but not limited to)

- the source (or apparent source) of the data
- delivery management based upon elements of HTML code within the file
- the display of certain content within a message
- the ability to follow certain classes of hyperlink from within a message

In managing such filtering rules, the University will always seek to facilitate the free flow of primary-purpose content while protecting against vexatious content and such , adjudicating based on the balance of risk. In respect of facilities provided by the University but managed on behalf of the University by a third party, the relevant third party may apply its own countermeasures for like purpose.

## 10.3 Industry-standard and best-practice procedures

The University does not exist in a vacuum, untouched by others. Network practices and procedures are constantly being re-established, and evolve as understanding grows of good practice or, conversely, as threats and risks take advantage of loopholes which become bad practice. The University, to maintain its reputation as a responsible network user, will instigate measures to encourage good practice and to inhibit poor practice.

In taking such measures, the University will have regard to industry-standard and best-practice procedures, tempering them with local variation if essential local requirements would be rendered impossible by the instigation of standard practice *in toto*. Local custom and practice (where alternative methods exist) will not be sufficient *per se* to cause best-practice solutions to be abandoned. Brunel University London cannot be held responsible for any loss or damage consequent upon the reasonable application of such countermeasures.

---

## 11 Professional immunity

In the course of maintaining the Brunel University London data network, staff of the Computer Centre (and certain other staff approved by the Director of the Computer Centre to assist in the process) may require to undertake activities which would otherwise fall outwith the provisions of the Policies of Brunel University London. Users should be aware that, subject to any external restrictions placed upon such activities (e.g., by legislation), staff involved in a *bona fide* investigation or technical operation will enjoy professional immunity against any technical infraction committed as a necessary part of such work. Any information or intelligence gained under such immunity is privileged, and the use of such information beyond the strict limitation of the task in hand will be considered a matter for the disciplinary procedures of Brunel University London.

## 12 Qualification of access permission

Users should be aware that Brunel University London retains the right to impose qualifications and restrictions on any permission to access a network account, whether temporarily or permanently, and without notice where the situation demands it.

Such qualifications and restrictions may be made

- in conjunction with other Brunel University London activities.
- in connection with a programme of service maintenance, change or enhancement.
- in response to any information relating to a threat to the security or smooth operation of the Brunel University London data network or any other Brunel University London service.
- at the discretion of the Director of the Computer Centre for any appropriate cause or reason.

Brunel University London will not be liable for any consequential loss suffered as a result of any such qualification or restriction.

## 13 Security

Confidentiality of data held within Brunel University London networked filestore cannot be guaranteed. It is the responsibility of each account-holder to exercise due judgment when dealing with sensitive issues — extreme caution should be taken when using a network account to store data or to transact business of a confidential or sensitive matter (e.g., personal information relating to health, disability and criminal record). Backup files are kept under the control of Brunel University London for the sole

purpose of disaster recovery and business continuity on a system-wide basis: they are not regarded as an 'offline repository' in any capacity, nor as a backtracking facility for the restitution of individual files following a reconsideration of the wisdom of any editing or disposal.

In terms of formal security gradings of UK government data, the Brunel University London data network and its attendant systems have not been declared qualified to store or manage data classified at a security grading higher than *Restricted*.

## 14 Data protection and retention

Any non-deleted file which contains personal information (as defined by the Data Protection Act 1998) comes within the requirements of that Act, and therefore may be disclosed on request to the subject of that information.

Data which, in accordance with good record-keeping practice, have been deleted from primary storage (and, where relevant, from Brunel University London archive storage) before a request is received under such auspices as Data Protection and Freedom of Information legislation will not, in the context of such a request, be retrievable from backup files held for the purposes of disaster recovery and business continuity.

Responsibility for data protection, and for aspects relating to disclosure under freedom of information legislation, rests with the Governance, Information and Legal Office of Brunel University London: if an account-holder has any doubt about any matter relating to such legislation, it is the duty of that account-holder to seek confirmatory approval from that office before any steps are taken in relation to such data.

## 15 Accounts with extended privileges

### 15.1 Introduction

The Computer Centre may provide a member of staff who requires elevated access privileges with an additional network account from which such actions may be carried out in a standard auditable way. Examples of such an account would be a *technical administrator account* (or *ADM account*) or a database administrator account (or *DBA account*). Where this policy refers to an extended-privilege account in general, it will be called an *EP account*.

By this means, if an EP account-holder's standard network account becomes compromised, then these additional privileges are not also compromised. It also means that this additional access can be quickly stopped (by disabling the EP account) without disabling the standard account (which would result in the staff member being cut off from e-mail, etc.).

An EP account may allow the account-holder to undertake such tasks (as appropriate to the account type) as

- adding a PC to the domain.
- logging onto a PC as a local administrator.
- logging onto a server as a local administrator.
- editing a group policy within a specific organisational unit (OU).
- acting as a domain administrator.
- performing high-level database administrative operations (e.g., creation, shutdown or recovery, and execution of OS system commands).
- ability to access fully a database's base tables, views and data dictionary.
- ability to access to a database instance even when the database is not open.
- ability to change a database's security settings.

An EP account only has the additional access to allow that staff member to undertake the extra tasks which require the privileges associated with the account; they do not have e-mail, filestore space or roaming profiles. An EP account will have appropriate audit-trail assurance built into its parameters. This will allow monitoring and investigation of account use, covering such areas as accountability, deterrence, management notification, and activity audit. This policy covers *all* EP accounts, whether issued to a member of staff in the Computer Centre or in any other unit of the University.

## 15.2 Requesting an EP account

Each EP account requires sponsorship by a senior staff member before being considered for creation. This will normally be the Team Leader of the requester's IT servicer, but may be an appropriately senior line manager if there is no Team Leader. The sponsor must ensure that the permissions being requested are reasonable, and will be the point of confirmation that the EP account is still necessary for operational purposes at periodic review.

The sponsor must inform the Computer Centre immediately the EP account is no longer required to be held by the account-holder, by e-mail to [computing-support@brunel.ac.uk](mailto:computing-support@brunel.ac.uk) in the first instance.

## 15.3 Approving and creating an EP account

An EP account will be considered and (if approved) subsequently created under the authority of the Systems Manager of the Computer Centre, who may delegate parts of the process appropriately. For example, authorities regarding ADM accounts may be devolved to a member of the Systems team; for DBA accounts, authority may be devolved to the principal Database Administrator within the Computer Centre.

In order to avoid any potential conflict of interest, the approval of an EP account for any member of the Systems team must be endorsed *a priori* by the Assistant Director (Technical Services) of the Computer Centre or by her/his line manager. Similarly, the approval of a DBA account for the principal Database Administrator must be endorsed *a priori* by the Assistant Director (Governance and Corporate Services) within the Computer Centre, or by his/her line manager.

## 15.4 Using an EP account

An EP account is not simply another account: the privileges granted for use imply a greater degree of trust in the account-holder. For this reason, the scope of use of an EP account must be more stringent than for a standard account.

- The EP account must have a strong and secure password. As for all accounts, this password must not be shared with anyone else. Failure to abide by this instruction will be considered a serious lapse of discipline.
- The EP account must be used only for the tasks approved at the time of the account's creation. Any abuse of this account may result in it being disabled with no warning to the account-holder, who may be subject to disciplinary proceedings.
- The use (or attempted use) of an EP account by anyone other than the account-holder (including the holder of another EP account) may result in disciplinary proceedings.
- The EP account should only be active during the time needed to carry out the required tasks. Leaving an EP account logged into a PC or server beyond such minimum time will be considered a serious lapse of discipline.

Each member of staff who carries an EP account will automatically be added to the Computing Contacts mailing list and to that staff group. This list/group is a primary means of communication regarding the University's IT service to key IT staff.

The use of an EP account is subject to all other policies, rules and regulations of the University: <https://intra.brunel.ac.uk/s/cc/Pages/Policies.aspx> contains copies of those policies managed by the Computer Centre.

## 15.5 EP account review

Because of the heightened privileges accorded to an EP account-holder, there must be clear procedures for review of an EP account. The principal reviewer of an EP account will be the account sponsor, working in conjunction with the Systems Manager within the Computer Centre (who has overall authority in these matters) and, in the case of a DBA account, with the principal Database Administrator within the Computer Centre.

There will be an overall periodic review of EP accounts: on an annual basis, each sponsor will be required to confirm, for each EP account under her/his sponsorship, that the account is still necessary

for operational purposes. The sponsor will have twenty working days to confirm an account, after which it will be disabled.

If the holder of an EP account changes role in any way, a particular review will be triggered. It is the joint and several responsibility of the sponsor and the account-holder to inform the Computer Centre (by e-mail to [computing-support@brunel.ac.uk](mailto:computing-support@brunel.ac.uk) in the first instance) of any such change of role as soon as such change is known to either party (*i.e.*, without waiting for the actual change date). The Computer Centre will also take notification of a change of role from HR as a trigger for a review.

## 15.6 EP account disablement

Because of the enhanced privileges accorded to an EP account, the Systems Manager within the Computer Centre (or a nominated deputy) has the authority to disable any EP account at any time, without notice, if he/she has reasonable cause to suspect a potential compromise of the integrity of the University's IT service, or any part thereof.

In the event of the sudden departure of a holder of an EP account, it is the duty of the sponsor to inform the Computer Centre (by e-mail to [computing-support@brunel.ac.uk](mailto:computing-support@brunel.ac.uk) in the first instance) without delay, and the account will be disabled forthwith. The Computer Centre will also take notification from HR of such a departure as a trigger for disablement.

## 16 Responsibility

Responsibility for account use rests with the individual, and all the way along the management/supervisory chain<sup>16</sup>: for the sake of conciseness, within this section, the term *manager* is to encompass anyone who has a managerial, supervisory or educative relationship with individual account-holders. Beyond that, it is also the responsibility of each user to encourage high standards of legal, technical and moral compliance in all other users, and to report any lapse from these standards to the Computer Centre, who will assess any need to restrict or suspend access by the offending party.

### 16.1 Responsibility of individual account-holders

Each user is responsible and accountable for the management of all data held in filestore associated with any account issued to that user or for the use of that user. Each user of a network account at Brunel University London has a duty of care to

- maintain security of access details and credentials to current standards as set out by Brunel University London.

---

<sup>16</sup> to include tutors and supervisors of students, and the academic management chain above such people

- ensure the practice of appropriate and proper use and management of data, including records management.
- understand all responsibilities with regard to data use and management.
- maintain current awareness of policies, practices, threats and problems relating to data use and storage at (and where relevant, beyond) Brunel University London.
- maintain up-to-date knowledge of Brunel University London's filestore management software as it evolves, and take full advantage of its facilities to aid the use, management, storage and retrieval of data.

The Senior Officer of each unit of the University is responsible for ensuring that each member of staff within that unit is aware of this network account policy, and of any changes made to it, and that each abides by it at all times.

Each student must realise that enrolment at Brunel University London confers a duty to follow the Policies and regulations of Brunel University London at all times, and to validate the integrity and parsimonious use of filestore on a regular and timely basis. The Senior Officer of each academic unit of the University has a duty to ensure that the students within that unit maintain awareness of their responsibilities in respect of network account management.

## 16.2 Responsibility of managers

### ***16.2.1 Managerial responsibility in respect to individual compliance***

The responsibility of the individual Brunel University London account-holder is laid out above: there is a corresponding responsibility of the management/supervisory chain to ensure compliance throughout the chain to the individual level.

It is the responsibility of anyone in a supervisory, managerial or educative position to

- ensure individuals' compliance with responsibilities at all times.
- provide adequate awareness, training and education (refreshed and updated as appropriate) for all individuals for whom the manager has chain responsibility.
- undertake risk assessment in order to establish appropriate levels of access, and appropriate confirmatory checks which are to be placed into procedural workflow to ensure that individuals' access and use meet Brunel University London's standards and values in such respect.

### ***16.2.2 Managerial responsibility in data access and management***

There may be occasions when it is necessary for a duly authorised member of Brunel University London to access data from an individual's filestore — most of such occasions will have been covered already under the appropriate sections of this Policy.

---

In the case of normal business use, where there is no reasonable possibility that sensitivity of the data being handled may be encountered, or that there may be sensitivity pertaining to any of the parties involved, the Senior Officer of the relevant unit of the University will make the access or will grant access to data within the filestore of staff or students within that unit.

In any case where sensitivity may be present, the Senior Officer of the relevant unit of the University should refer third-party access matters for adjudication

- to the Head of Registry in regard to academic matters relating to students.
- to the Chief Operating Officer in regard to non-academic student matters.
- to the Director of Human Resources in regard to non-student matters.

The Director of the Computer Centre will have discretionary powers to grant access in the absence of the appropriate authority in any of the above instances, taking advice if necessary from the Governance, Information and Legal Office of Brunel University London.

## 17 Disciplinary procedure

In the event of an apparent breach of the Brunel Acceptable Computer Use Policy, of this Policy, or of a related Policy by a user or group of users, the Director of the Computer Centre, or his designated agent, has the authority to withdraw access to the facilities from any user in summary fashion. Recourse will be made to Brunel University London's usual disciplinary procedures where it is deemed necessary by the Director of the Computer Centre. Furthermore, Brunel University London may take legal action in any instance that such a course of action is deemed to be in the interests of Brunel University London.