



## **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 the University. 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 the University and beyond, taking due consideration of legal precedent, and having due regard to the practices and experiences of our colleagues in other institutions.

**August 2009**

## **Document properties**

### **Authority**

Director, Computer Centre

### **Sponsor**

Director, Computer Centre

### **Responsible officer**

Policy Development and Quality Manager, Computer Centre

### **Recent version history**

Current version, August 2009, is derived from and supersedes version published in May 2005.

# 1 Introduction

The University must clarify how any network computer account granted by Brunel should be used and managed by the account-holder, whether he/she be a student, member of staff, or other affiliated person.

Each user must abide by all relevant external and internal regulations, and must act in the overall interested 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 the University, and the assurance of its continuity, having due primacy.

This Policy sets out the accepted management of accounts on the University'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 the University 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>.

## 2 Supervening policies and frameworks

This policy describes the local rules by which business is transacted using a network account, but such use must also comply with laws, 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 network is subject to the provisions of the Brunel Acceptable Computer Use Policy (BACUP). The text of BACUP may be found with other such documents at <http://www.brunel.ac.uk/about/administration/policy/> and is contained within the Student Handbook. This forms part of the University's rules.

### 2.2 Joint Academic Network(JANET)

The University'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 may be put — this obviously includes our use of network access beyond Brunel. 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

---

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

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

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 network, and it is at all times the individual user's duty to be aware of what constitutes legal use and behaviour.

## 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.

# 3 Components of network account management

It is useful to make sure that everyone is agreed on some definitions and forms of usage: this section sets out the ways in which we use certain terms within the context of the University's network account service.

## 3.1 Network account

A *Brunel network computer account* (within this Policy called an *account*) is the means by which a registered Brunel user may carry out business using computers connected to the Brunel University Data Network for the creation, storage, analysis and management of data (not restricted to numeric data) using networked computers within the parameters set by the Brunel Acceptable Computer Use Policy (BACUP), other relevant Brunel University Policies, Rules and Regulations, and supervening laws. Indeed, this account is the only official means of conducting Brunel business electronically or with recourse to networked electronic devices, whereby these business data contribute to the official records of the University. It is therefore critically important that staff and students use their Brunel 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 visiting a Computing Support office with the user's University 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 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)<sup>4</sup>, so is not considered to be secret. Notwithstanding, each account-holder has a duty of care in avoiding unnecessary promulgation of Brunel usernames through inadequate security of action. In particular, these must not be divulged to a third party beyond Brunel except with the express permission of the Director of the Computer Centre.

---

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

<sup>4</sup> indeed, this structure is the sole mail address for a student account

### 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 of any such actual, suspected or potential compromise from any reputable source, 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 data. Following any such action, the account-holder must attend the Computing Support office 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 Data Network, any transgression may lead to disciplinary proceedings appropriate to a serious breach of University regulations.

### 3.4 Filestore

A 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.

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 (floppy disk, CD, DVD, USB memory, etc.): as with networked filestore, the responsibility to comply with all relevant legislation and policies remains with the account-holder.

### 3.5 Primary purpose of network account

The reason for issuing a Brunel network account is to offer the account-holder access to facilities which further the academic or corporate business of the University. 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 contact data, 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 the University, or any applicable legislation 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.

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 staff**

A member of Brunel staff 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 staff status rests with the Director of Human Resources.

### **4.1.1 Permanent**

As soon as possible after arrival at Brunel, 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, 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 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, 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 Data Network on that date. The issue of an account to a temporary member of staff will require that the appropriate Head of School (or analogous 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 the University'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 the University, with appropriate credentials (including approval of the Head of School or analogous unit within 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 the University. 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 Data Network on that date. The issue of an account to a volunteer member of staff will require that the appropriate Head of School (or analogous 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 the University's compliance with legislation and records management practice.

It is the responsibility of the Head of School (or analogous unit within the University) to inform the Computer Centre of any change to the status of the volunteer, or to the agreed period of access.

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

On retirement from active Brunel University 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 may be granted the use of a new account for the purpose of maintaining contact (principally by electronic mail) with Brunel. The status of a retired member of staff will preclude, due to widespread licensing restrictions, the use of much University-licensed software.

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

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

### **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 the University 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 or 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, 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 the University, *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 the University should be set up as an appropriate (probably temporary or fixed-term) staff account. The principal focus for such support workers will be the University's Disability and Dyslexia Service.

## **4.2 Brunel student**

A student duly registered on a course of study at Brunel University 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 the University by applicants to create accounts for expected registrands, these accounts to be enabled at the time of University registration. However, the formal start of account creation begins following registration, and the enabling of a student account is contingent on appropriate University registration.

In any instance of a student's progression from one course of study at Brunel University 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.

### **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, 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 the University 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, 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 the University's process of Registration during the allotted time for the

---

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

course cohort's attendance, on the production of the account-holder's currently-validated University ID card (or an unvalidated University 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 Computing Support office within the Computer Centre, 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 the University'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, 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, 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 the University's process of Registration during the allotted time for the course cohort's attendance, on the production of the account-holder's currently-validated University ID card (or an unvalidated University 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 Computing Support office within the Computer Centre, 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 the University'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, 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, 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 the University's process of Registration during the allotted time for the course cohort's attendance, on the production of the account-holder's currently-validated University ID card (or an unvalidated University 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 Computing Support office within the Computer Centre, 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 the University'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, 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, a student becomes entitled to an account associated with that course of study, for the duration of that course of study. After completion of the University's Registration process, account details will be issued to the account-holder at the Computing Support office within the Computer Centre 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 the University'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, 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.

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

A full-time student will have account access rights in accordance with University Policies 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 University Regulations and Policies.

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

A part-time student will have account access rights in accordance with University Policies 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 University Regulations and Policies.

### **4.2.8 Continuous professional development**

A student who undertakes modular study at Brunel University 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 the University's Registration process for the module, account details will be issued to the account-holder at the Computing Support office within the Computer Centre on production of the account-holder's currently-validated University 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, 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 student will have account access rights in accordance with University Policies 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 University Regulations and Policies. Rights of connection to the Brunel University Data Network, or of access to data held therein or elsewhere, from a connection-point

which is not owned or managed by Brunel University<sup>6</sup>, is entirely at the discretion of the owner/manager of that connection point. See also *Student undertaking work for the University*.

#### **4.2.10 Former student**

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

#### **4.2.11 Student undertaking work for the University**

If, during a course of study, a student undertakes work (whether or not for reward) for the University, 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 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 the University 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 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 the University, gain delegate access *in loco studentis* to the student's account. The support worker's own business with the University should be carried out using an appropriate staff account (see appropriate sections under *Brunel 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 makes beneficial more general access rights than may be extended to other external bodies.

#### **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.

---

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

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

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 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 the University. The characteristics of the account may differ from those of an account issued to an analogous member of staff of the University, 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 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 the University. 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**

The University recognises certain trades unions as representative bodies for groups of staff within the University. Though these are third-party organisations (and therefore do not fall within much of the licensing structure of the University'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 the University.

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 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 the University from taking action (including disciplinary action) in the event of inappropriate usage of such an account.

### **4.4.1 Elected local officer of a Brunel-recognised trade union**

At the discretion of the Director of the Computer Centre, a member of staff at Brunel University, having been elected as an officer in a Brunel branch of a Brunel-recognised trade union, 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 the University, 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 *Brunel staff as officer at another level of a Brunel-recognised trade union***

There is no entitlement to an account for a member of staff of Brunel University who holds an office in a Brunel-recognised trade union where the duties associated with that office extend beyond activity carried out on behalf of its members employed by Brunel University.

#### **4.4.3 *Non-Brunel officers of a Brunel-recognised trade union***

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

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

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.

### **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 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.

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

A member of staff from another academic institution may be contracted to undertake work for the University<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 the letter of contract 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 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 appropriate Head of School (or analogous unit within 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.

---

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

In general, such an account is likely to have restrictions placed upon it to ensure the University'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 Contractor company staff**

On occasion, it may be beneficial that a named member of staff of a company contracted to undertake work for the University should have an account on the Brunel University 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 Computing Support office. 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.

In general, such an account is likely to have stringent restrictions placed upon it to ensure the University'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.

#### **4.5.3 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 Data Network for specific purposes of supporting the University'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 Computing Support office. 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. 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 the University'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.

#### **4.5.4 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 the University 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 the University is entitled to an account in order to facilitate Council business. Such an account will have the Secretary to the Council of the University 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.

### **4.7 Associated persons**

In addition to staff and students of the University, there are several classes of person who may be designated as 'associated' with Brunel. Sponsorship of associates' accounts may be devolved within the formal sponsor's hierarchy with the agreement of the Director of the Computer Centre.

#### **4.7.1 Professor Emeritus**

A Professor Emeritus of Brunel University is entitled to an account for the purposes of maintaining academic communication with Brunel University. The account will be issued by the Computer Centre for a fixed term (renewable), 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.

#### **4.7.2 Fellow of the University**

At the discretion of the Director of the Computer Centre, a person granted a Fellowship of the University may be issued with an account for the purposes of facilitating communication between the Fellow and the University. The account will be issued by the Computer Centre for a fixed term (renewable), 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.

#### **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), 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.

#### **4.7.4 Exchange student**

A student of another institution who is enrolled on a course of study within Brunel University on an exchange basis as part of an award of the other institution is entitled to an account on the Brunel University Data Network with characteristics appropriate to such status. The student should apply to the Computing Support office within the Computer Centre, with a currently-validated Brunel 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, as indicated by the appropriate information within Brunel University'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.

#### **4.7.5 Student of associated institution — Brunel-validated award**

A student of an associated institution who is enrolled on a course of study for an award which is validated by Brunel University is entitled to an account on the Brunel University Data Network with characteristics appropriate to such status. The student should apply to the Computing Support office within the Computer Centre, quoting the Brunel University Student Number as entered in the Brunel Student Records system, and an identification from the associated institution. 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'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.

#### **4.7.6 Student of associated institution — locally-validated award**

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 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 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 appropriate Head of School (or analogous 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.

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

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 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 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 appropriate Head of School (or analogous 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.

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

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<sup>9</sup> may be granted an account on the Brunel University Data Network. 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 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.

In general, such an account is likely to have stringent restrictions placed upon it to ensure the University'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 the day-to-day pressures on its facilities, and by the University's need to comply with legislative and licensing restrictions.

---

<sup>9</sup> for example, a tenant company of the Science Park

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

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

A member of staff of another academic institution who is visiting Brunel University for an extended period may, at the discretion of the Director of the Computer Centre, be granted an account on the Brunel University Data Network for an agreed fixed period. This will require the support of the appropriate Head of School (or analogous 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. 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 the University'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 (for example, a teacher, administrator or student at a summer school located at Brunel University) has no entitlement to an account on the Brunel University 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: 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 and legislation. 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 the University's compliance with legislation and records management practice. In particular, access to licensed software may be limited.

#### **4.8.3 Non-Brunel student**

There is no general entitlement to an account on the Brunel University 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 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 Data Network. Permission is unlikely to be granted if there is an alternative means whereby the student may communicate with the home institution.

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

### **4.9 External account-holder**

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

### **4.9.1 Audit or analogous function**

As part of the standard function of audit, inspection or validation of any part of the University<sup>10</sup>, it may be necessary for external persons to gain access to the Brunel University 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 will co-operate with the investigative body concerned to optimise the appropriate access, and will agree terms and conditions for account management accordingly.

### **4.9.2 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.

## **5 Acceptable categories of use**

The University provides ICTS<sup>11</sup> facilities (including network accounts) for use in the furtherance of the learning, teaching, research and approved business activities of the University: activity which conforms to the above is defined as 'primary-purpose use'. The University's facilities should not be used for

- personal use at a level which has the potential to impinge on primary-purpose use of University facilities
- the use or storage of unsolicited commercial, advertising or petitioning material (including any such mail in conjunction with charitable organisations or purposes).
- the unauthorised use by a third party of confidential material concerning the activities of the University.
- 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.
- any activity likely to harm the reputation of the University or the goodwill extended to the University.

In all cases and at all times, the account-holder is bound by the Brunel Acceptable Computer Use Policy<sup>12</sup> while using the facilities offered by or through the Brunel University Data Network.

---

<sup>10</sup> for example, a QAA inspection of a subject discipline

<sup>11</sup> Information and Communications Technology and Services

<sup>12</sup> available at <http://www.brunel.ac.uk/about/administration/policy/>

## 6 Ownership, custody, agency and disclosure

### 6.1 Ownership

All data created and maintained on computer systems within the Brunel University Data Network become the sole property of Brunel University, unless there is an explicit agreement to the contrary agreed by the University. The University 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 the University or of financial loss to the University, or to maintain the reputation of the University. The University 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.

### 6.2 Official record of the University

Data which contribute to the academic or corporate business of the University become part of the corpus of official records of the University. For this reason, such business must be transacted using the official account(s) provided by the University for the purpose. 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. The data, once created, edited or otherwise used, become subject to University records management policies and will, where relevant, become available for lawful disclosure to third parties (for example, under Freedom of Information legislation).

### 6.3 Personal use of the account

The University 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 a third party.
- does not conflict with the University's rules, regulations, policies and procedures
- is not of a nature that conflicts with the business of the University
- is not of a nature which could lead to a diminution of the University'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 account.

### 6.4 Monitoring data

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

- required by law
- for the purposes of maintaining the free flow of primary-purpose business
- as part of an investigation of a suspected violation of the ordinances, rules, regulations or policies of the University.

The University'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>13</sup>.

## 6.5 Custody of data

Responsibility for safe and secure custody of data stored within the Brunel University Data Network lies with the file owner<sup>14</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 the filestore associated with the account, 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 the University, 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 the University. Advice will be sought from the Office of the Secretary to Council where there is any doubt about the legitimacy of disclosure. In support of the lines of authority for disclosure as laid down below, the Director of Resources and Operations and the Vice-Principal 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 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).

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

First and foremost, it should be noted that all data held within an account are deemed to be 'business data'. 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.

Authority for the release of business data to be disclosed to a third party is vested initially in the normal line management of the University, and alternatively (and directly in the case of disclosure from a student account) in the Head of School (or analogous 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.

---

<sup>13</sup> See, for example, <http://www.archive.official-documents.co.uk/document/parlment/nolan/nolan.htm>

<sup>14</sup> file ownership is independent of the ownership of data

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

- the appropriate Head of School, in the case of disclosure from a Brunel student account (*i.e.*, one classified within the subsections of accounts under ***Brunel student***)
- the Director of Human Resources, in the case of disclosure from any account other than a Brunel student mail 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 network account: these are

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

### 7.1 Access to a network account

An account-holder's primary mode of access to a network account will be via a workstation which is connected to the Brunel University 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 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 business or to the integrity of Brunel data or computing 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 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 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, 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 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.

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 business or to the integrity of Brunel 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 a Brunel 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.

## 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 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 the University, 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.

### 8.1 Agent

Perhaps the most well-known instance of delegation within an 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 the University of data simultaneously made available to all members of a peer group<sup>15</sup>. In the management of such data, the group members must always ensure that they act on behalf of the

---

<sup>15</sup> such as **computing** support

group. Each member of the group bears the responsibility to maintain group records, but the supervisor or other 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 principal's Head of School (or analogous unit within 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 Head of School), 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 Director of Resources and Operations and the Vice-Principal have authority to act in the absence of primary authorities, as do, *in extremis*, the Director of the Computer Centre and Secretary to Council.

## 8.5 Technical investigation

A user may, through a service enquiry, request a technical investigation which must result in access to that user's data: 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 a mail account-holder may be given by any one of the following investigative authorities, *viz.*

- the Vice-Chancellor
- the Director of Resources and Operations
- 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 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 the University.

## 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 the University<sup>16</sup> and with the appropriate Head(s) of School(s).

### 9.1 Business or academic continuity

If the academic or business continuity of the University is put at risk by the inability of an account-holder to manage an account or data therein, the Head of School (or analogous unit within 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 Head of School 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 any Head of School.

### 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.

---

<sup>16</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 of these managers may be involved in the case of staff access to a student account

## 9.3 Internal disciplinary process

Data held within the Brunel University 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 Director of Resources and Operations.

## 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 the University 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 Managing Director (Resources and Operations)
- 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 the 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
- 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 the University.

## 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 the University 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 the University's academic and corporate business, and in the safeguarding of the University's reputational integrity, the University 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 the University, but it is recognised that automatic filtering, however efficient, remains an inexact science.

### 10.1 Countermeasures against vexatious matter

The University will deploy countermeasures against the attempted infiltration of the Brunel University Data Network by vexatious matter from whatever source or apparent source.

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

The University 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.

## 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 is keen to maintain its reputation as a responsible network user, and will instigate measures to encourage good practice and to minimise threats and risks arising out of 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.

## 11 Professional immunity

In the course of maintaining the Brunel University 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 University's Policies. 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.

## 12 Qualification of access permission

Users should be aware that the University 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 University 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 Data Network or any other Brunel service
- at the discretion of the Director of the Computer Centre for any appropriate cause or reason

The University 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 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 the University 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 BUDN 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

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 University 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.

## 15 Responsibility

### 15.1 Responsibility of individual users

Each user is responsible and accountable for the 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 has a duty of care to

- 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
- maintain up-to-date knowledge of Brunel'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 Head of each School (or equivalent group within the University) is responsible for ensuring that each member of staff 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 the University confers a duty to follow the University's Policies and regulations at all times, and to validate the integrity and parsimonious use of filestore on a regular and timely basis.

The Senior Tutor of each School has a duty to ensure that the students within that School maintain awareness of their responsibilities in respect of network account management.

---

## 15.2 Responsibility of managers

There may be occasions when it is necessary for a duly authorised member of the University to access data from an individual's filestore.

In the case of normal business use, the Head of School (or equivalent group within the University) will make the access or will grant access to data within the filestore of staff or students within the School (or similar) concerned.

In sensitive cases, the Head of School (or equivalent) should refer matters regarding access to student filestore to the Director of Resources and Operations in cases involving non-academic matters, and to the Head of Registry in cases involving academic matters, for adjudication on access to data.

In sensitive cases relating to a member of staff, the Head of School (or equivalent) should refer the matter to the Director of Human Resources for adjudication on access to data.

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 Office of the Secretary to Council.

## 16 Disciplinary procedure

In the event of an apparent breach of any of the Brunel Acceptable Computer Use Policy or of this Policy by a user or group of users, the Director of the Computer Centre, personally or through a designated agent, has the authority to summarily withdraw access to the facilities from any user. Recourse will be made to the University's usual disciplinary procedures where it is deemed necessary by the Director of the Computer Centre. Furthermore, the University may take legal action where necessary.