



## **Information Strategy**

### **Electronic mail policy**

The purpose of this document is to lay forth the policy which regulates the use of electronic mail 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 electronic mail should be used and managed by everyone within Brunel, as there is a common misconception that electronic mail messages are informal and/or ephemeral in nature.

At Brunel, electronic mail is recognised as a formal communication medium for University transactions, including communication with students, and therefore needs to be managed like all other University records. A key aspect of such management is the Brunel Central Archive (BCA).

This Policy sets out the accepted use and management of the University's electronic mail services and facilities: in conjunction with our guidelines of good practice, it will enshrine good management practice and will help to ensure that the University is compliant with all relevant legislation.

## 2 Supervening policies and frameworks

This policy describes the local rules by which business is transacted using electronic mail, but mail 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 relevant policies and 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>1</sup>. This limits the use to which the access from the University to the Internet may be put — this obviously includes our use of electronic mail 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 mailflow and communication for all users.

### 2.3 English law

Clearly, all that we do must comply with English law, and our use of an electronic mail account is no exception. It therefore follows that, in addition to any ICTS-specific legal duty which is set out in appropriate specific legislation, there is a constant and inflexible duty laid upon each user and upon any grouping of users to abide, jointly and severally as relevant, by all relevant Acts of Parliament and similar legal instruments at all times while connected (or attempting to make a connection) to the Brunel mail and messaging facilities, and it is at all times the individual user's duty to be aware of what constitutes legal use and behaviour.

---

<sup>1</sup> See <http://www.ja.net/documents/publications/policy/aup.pdf>

## 2.4 Supranational jurisdictions

Over and above English law, we must always act within European and international law as we transact business using electronic mail.

## 3 Components of mail use

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 electronic mail service.

### 3.1 Brunel electronic mail account

A *Brunel electronic mail account* (within this Policy called a *mail account*) is a subsidiary service account within the parameters of the account-holder's *Brunel network computer account*.

It is the means by which a registered Brunel user may carry out Brunel business by electronic mail 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 mail account is the only official means of communicating Brunel business, whereby these business messages become official records of the University. It is therefore critically important that staff and students use their Brunel mail accounts for this business, and that regular and frequent access is made by each student and member of staff to this mail account to check for incoming mail which may contain Brunel business.

Access is made to the mail 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 reset a forgotten password must be made by visiting a Computing Support office with the user's University ID card as proof of identity.

The mail account is defined by the *mailname* assigned by the Computer Centre: this is the same as the username for students (other than research postgraduates), and is as given<sup>2</sup> by the Computer Centre to research postgraduates, staff and others. The user's *electronic mail address* is formed using the mailname, the full format being *mailname@brunel.ac.uk* (case-insensitive).

### 3.2 Post-holder aliases and mail-lists

Much of Brunel's mail is really sent to a post-holder rather than an individual — even if the individual's name appears as the addressee. The continuity of our business is at risk, though, when someone moves on, unless we actually use a post-holder alias (such as *data.protection@brunel.ac.uk*) to convey messages to the post-holder. Furthermore, we must be able to distinguish between messages sent to the person *as an individual* and those sent to the person as a post-holder.

For these reasons, it is considered good practice at Brunel to use, wherever appropriate, a post-holder alias in electronic correspondence.

Where mail is sent to a group of people (such as the Computing Support team), it is appropriate that the group mail-list (in our example, *computing-support@brunel.ac.uk*) is used throughout the conversation<sup>3</sup>. In particular, the practice of restricting later parts of a message-thread to an individual within the group, freezing out other group members from group business (and thereby from the increase in common group knowledge), is deprecated most

<sup>2</sup> normally the user's name in the format *firstname.lastname*

<sup>3</sup> through strict use of the group mail-list in the *To* and *Reply-to* fields when sending and replying respectively

strongly. An exception may be made when an individual may, with the consent of the group, take a matter ‘off-group’ before making a full report back to the group, but this should really be exceptional behaviour.

These elements of good practice are stressed in order that threads and conversations are not ‘lost’ due to any absence (or distraction) of an individual.

### 3.3 Brunel mail system

When we refer to *Brunel’s mail system*, we mean the servers and software located in the University which contribute to the delivery, flow, accessibility and storage of mail, and to the services which contribute to the ability to carry out Brunel mail business from elsewhere. This includes the Brunel Central Archive (BCA) of messages sent to or from a staff electronic mail account.

### 3.4 External and internal mail

Mail which operates wholly within the Brunel mail system is considered to be internal mail. The accessibility of the Brunel mail system from beyond campus boundaries makes the definition of internal mail independent of geography: for example, a message sent from one Brunel mail account to another using Brunel’s *Outlook Web Access* service is considered to be internal mail. Conversely, a message sent from or to a non-Brunel account, even if initiated and received within the campus, will be considered to be external mail.

### 3.5 Mailbox, storage and archive

#### 3.5.1 Mailbox

Messages sent to a mail account may be accessed through that account’s *mailbox*: this is the set of logical (rather than physical) locations from which an individual message may be opened. The account-holder may choose to superimpose managerial actions which may move or copy the access-point of a particular message (either on the explicit command of the account-holder, or by the application of message rules which test the satisfaction of logical criteria) from the primary entry-point (often called the *inbox*): in our terminology, the message remains within the *mailbox*.

In like manner, a message which is sent by the account-holder may generate a copy for the sender — the primary access-point is often called the *sentmail* folder. The copy of the sent message remains within the *mailbox*, whether or not its access-point is changed through explicit relocation or by the application of automatic message rules.

#### 3.5.2 Storage

Clearly, a message which remains within the Brunel mail system beyond the time of transmission is *stored* within the system. This policy endorses the terminology and concept of an account-holder’s “storage of a message”, even in the case that the account-holder only has maintenance control of the access-point to the message, or to some or all of multiple such access-points<sup>4</sup>.

---

<sup>4</sup> a message sent to multiple addressees at Brunel may only be stored once, with an access-point for each addressee; alternatively, an account-holder may create (by copy or search-group) multiple access-points to the same stored message

### 3.5.3 Archive

While a message is in a mailbox, it is immediately available for use by the account-holder<sup>5</sup>. At a later stage, the message may be removed from the mailbox, to be accessible from BCA. It is important to recognise that accessibility is, generally speaking, unimpeded when a message transits to BCA-only status, though certain delegated powers may require specific configuration within BCA. It is important to note that the act of archiving a message forms part of the management of that message, and therefore falls within the University's Records Management policies.

Furthermore, a user may decide to move or copy a message into a file which resides beyond the reach of the University's messaging system (for example, as a text file in general filestore). This does not alter the status of the message in terms of any investigation or request for disclosure, and the University's Records management policies will continue to apply.

## 3.6 Message types

We have noted that each business message of the University has a certain status as a record of the University. In general, there are three types of message, *viz.*,

- an official message of the University is a message which is passed from one post-holder to another, or to a group of post-holders: it transacts University business which arises by virtue of the posts held (*e.g.*, from the Safety Officer to Heads of Schools, or from the account manager of a supplier company to a departmental administrator), irrespective of the identity of the individual incumbents
- an administrative message of the University is a message which transacts University business between an individual and a post-holder at the University, or which passes University business between an individual at the University and a post-holder. The crucial difference is that the individual is acting as an individual: for example, a message sent by a member of staff to an administrator enquiring about his/her current holiday entitlement is an administrative message.
- an individualised message transacts University business between two individuals (for example, an agreement between two members of a group to arrange task coverage).

## 3.7 Primary purpose of mail system

The reason we have a mail system at Brunel is to process messages which further the academic or corporate business of the University. This is known as the *primary purpose* of the Brunel mail system, and messages which qualify under the above umbrella are known as *primary-purpose messages*.

Primary-purpose mail must have priority at all times.

## 4 Entitlement to a mail account

The entitlement to a mail account is subsidiary to the entitlement to a network computer account, policy for which is described in the *University's network account policy*. Without access to a network computer account, there will be no ability to transact electronic mail business for that account. This policy describes entitlements specific to the transaction of electronic mail during the currency and validity of the supervening network computer account. 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.

<sup>5</sup> it may also be available for some or all forms of access and management by others within the University, dependent on the mail client being used and upon permissions granted by the account-holder

Users should note that the Computer Centre will manage demographic and other data relating to the mail 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 or other relevant Policies or legislation may include the total or partial suspension of network account access by an account-holder and a subsequent review of the period of such access on any resumption of access privileges.

## 4.1 Brunel staff

A member of Brunel staff will generally be issued with a mail account for the duration of a contract of employment or an analogous agreement, as part of the service accruing to a general network account. The authority for conferring current Brunel staff status rests with the Director of Human Resources.

The primary medium of access for such an account will be the University's supported mail client for staff use, on a PC which satisfies all the following criteria.

- The PC is located within a public-domain workarea or within an office or similar environment at Brunel University
- The PC is of a make and model approved by the Computer Centre as a standard-type PC for the purposes of accessing the Brunel University Data Network
- The PC has been configured with the image approved by the Computer Centre for use to access the Brunel University Data Network from the relevant location
- No modification has been made to the PC which might interfere with the ability to connect to any part of the Brunel University Data Network or to use any service associated with the use of the University's standard mail client in the standard manner

An attempt to use any other mode of access may encounter access restrictions.

The conferring of a staff account for electronic mail will normally generate a parallel presence within the Brunel Central Archive. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

### 4.1.1 *Permanent*

The mail account will be set up as part of the network account registration procedure, and will generally run for the duration of the network account. There will be no right of access to the mail account, nor to data associated therewith, by the account-holder following the termination of the network account. It is the responsibility of the account-holder and of the appropriate Head of School<sup>6</sup> (or analogous unit within the University) to discuss with the Computer Centre the arrangements for ongoing management of past and future messages to the mail account by another member of staff after the termination of the network account, otherwise all data pertaining to the account may be deleted from the Brunel University Data Network on that date. Such discussions should take place at least two months before the termination date.

### 4.1.2 *Fixed-term*

The mail account will be set up as part of the network account registration procedure, and will generally run for the duration of the network account. There will be no right of access to the mail account, nor to data associated therewith, by the account-holder following the termination of the network account.

---

<sup>6</sup> or, by agreed devolution, the School Manager

It is the responsibility of the account-holder and of the appropriate Head of School (or analogous unit within the University) to discuss with the Computer Centre the arrangements for ongoing management of past and future messages to the mail account by another member of staff after the termination of the network account, otherwise all data pertaining to the account may be deleted from the Brunel University Data Network on that date. Such discussions should take place at least two months before the termination date.

### **4.1.3 Temporary**

If a mail account is set up as part of the network account registration procedure, it will generally run for the duration of the network account. It is likely that the mailname for such a mail account will not be personalised, therefore the use of such a mail account for personal business is not appropriate. There will be no right of access to the mail account, nor to data associated therewith, by the account-holder following the termination of the network account.

It is the responsibility of the account-holder and of the appropriate Head of School (or analogous unit within the University) to discuss with the Computer Centre the arrangements for ongoing management of past and future messages to the mail account by another member of staff after the termination of the network account, otherwise all data pertaining to the account may be deleted from the Brunel University Data Network on that date. Such discussions should take place at least two months before the termination date. The issue of a mail 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 mail account and all compliance issues, and for the management of any data associated with the mail account at the dissolution of the account-holder's access rights.

### **4.1.4 Volunteer**

On occasion, work may be done for the University by an external person volunteering service (for example, an alumnus giving time for a School or administrative unit of the University): in certain such cases, a mail account may be needed.

If a mail account is set up as part of the network account registration procedure, it will generally run for the duration of the network account. It is possible that the mailname for such a mail account will not be personalised. For reasons of compliance and records management, the use of a mail account by a volunteer for personal business is not appropriate. There will be no right of access to the mail account, nor to data associated therewith, by the account-holder following the termination of the network account.

It is the responsibility of the account-holder and of the appropriate Head of School (or analogous unit within the University) to discuss with the Computer Centre the arrangements for ongoing management of past and future messages to the mail account by another member of staff after the termination of the network account, otherwise all data pertaining to the account may be deleted from the Brunel University Data Network on that date. Such discussions should take place at least two months before the termination date. The issue of a mail 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 mail account and all compliance issues, and for the management of any data associated with the mail account at the dissolution of the account-holder's access rights.

### **4.1.5 Retired staff member**

On retirement from active Brunel University service, the mail account held by a permanent member of staff will be closed. At the discretion of the Director of the Computer Centre, and following consultation with the Director of Human Resources, a retired member of staff who has been granted the use of a new account may also be granted an associated mail account. This mail account may be restricted in scope, and for reasons of compliance and records management, the use of a mail account by a retired member of staff for personal business other than the maintenance of contact with Brunel University is not appropriate.

---

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

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

### **4.1.7 Field testing**

The granting of a mail account in association with any network account set up for field testing will be dependent on the need for mail access as part of the field tests. The use of such a mail account for personal business, or for any purpose not intimately connected with the field tests, is inappropriate.

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

If a member of staff is enrolled as a student of Brunel University, then a mail account will be issued to that person in the capacity of a student on the appropriate course. This account will run concurrently with the staff member's post-related mail while the person enjoys dual status. It is important, and is the responsibility of the account-holder, to ensure the separation of these two mail accounts, the staff account being used for activity related to the account-holder's employment, and the student account for course-related activity. There will be no access to the student account after its termination.

### **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 mail account needed for administrative contact between the support worker *per se* and the University should be conducted through an appropriate (probably temporary or fixed-term) staff account. The principal focus for such support workers will be the University's Disability Service.

## **4.2 Brunel student**

A student duly registered on a course of study at Brunel University will be entitled to a mail account tailored to the class of registration, for the duration of the course of study, with the exception of certain short-term courses for which mail access is deemed unnecessary by the Director of the Computer Centre, following consultation with the appropriate Head of School (or analogous unit within the University).

In any instance of a student's progression from one course of study at Brunel University to another, there will be no entitlement of mail 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 mail accounts.

The primary medium of access for such an account will be the University's supported mail client for student use, on a PC which satisfies all the following criteria.

- The PC is located within a public-domain workarea at Brunel University
- The PC is owned and managed by the Computer Centre as a standard-type PC for the purposes of accessing the Brunel University Data Network
- The PC has been configured with the image approved by the Computer Centre for use to access the Brunel University Data Network from the relevant location
- No modification has been made to the PC which might interfere with the ability to connect to any part of the Brunel University Data Network or to use any service associated with the use of the University's standard mail client in the standard manner

An attempt to use any other mode of access may encounter access restrictions. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

### **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 mail usage, become entitled to use a mail 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 must not be used for personal business, or for any purpose not connected with the course-related usage. There will be no access to the mail account, nor to associated data, following the end of the prerequisite course.

### **4.2.2 Foundation**

On registration for an undergraduate course of study leading to a foundation award at Brunel University, a student becomes entitled to a mail account associated with the network account for that course of study, for the duration of that course of study. Mail account access will follow general network account access, but cannot precede it. 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 mail account appropriate to that course of study.

### **4.2.3 Undergraduate**

On registration for an undergraduate course of study at Brunel University, a student becomes entitled to a mail account associated with the network account for that course of study, for the duration of that course of study. Mail account access will follow general network account access, but cannot precede it. 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 mail account appropriate to that course of study.

### **4.2.4 Taught postgraduate**

On registration for an postgraduate course of study by teaching at Brunel University, a student becomes entitled to a mail account associated with the network account for that course of study, for the duration of that course of study. Mail account access will follow general network account access, but cannot precede it. 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 mail account appropriate to that course of study.

### **4.2.5 Research postgraduate**

On registration for an undergraduate course of study at Brunel University, a student becomes entitled to a mail account associated with the network account for that course of study, for the duration of that course of study. Mail account access will follow general network account access, but cannot precede it. 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 to any other status at the University, the student will receive a new mail account appropriate to that course of study.

---

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

A full-time student will have mail 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 mail 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) may, at the discretion of the Director of the Computer Centre and following consultation with the appropriate Head of School, be entitled to a mail account with characteristics appropriate to the learning outcomes of the module, for the duration of the module, if mail access is deemed necessary for the successful completion of the module. Such an account may be non-personalised in character, and therefore the use of such a mail account for personal business is inappropriate. Mail account access will follow general network account access, but cannot precede it. 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 may receive a new mail account as appropriate to the changed status.

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

A student will have mail 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>7</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 a mail 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, a mail account may, at the discretion of the Director of the Computer Centre and following consultation with the appropriate Head of School (or analogous unit within the University), be issued with a status appropriate to the work being undertaken<sup>8</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 mail 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.

---

<sup>7</sup> for example, from the workplace during placement

<sup>8</sup> this will normally be as a Brunel member of staff

---

### **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 a mail 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 mail account. The support worker's own correspondence with the University should be carried out using an appropriate staff mail 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 mail accounts: the Union is independent of the university, but its symbiotic status requires more general access rights than other external bodies.

There is no medium of access designated as primary medium for this class of accounts. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

### **4.3.1 Student as elected officer**

Each of the sabbatical offices has, at the discretion of the Director of the Computer Centre, the entitlement to a mail 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. The mailname is post-related and non-personal. Continuity is maintained through the sponsorship of these accounts by the General Manager of the Union of Brunel Students, assisted by the Human Resources Manager of the Union of Brunel Students.

For reasons of compliance and records management, it is not appropriate for the officer to use this account for personal business.

### **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 a mail 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.

### **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 a mail 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 a mail 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 mail account following its termination. For reasons of compliance and records management, it is not appropriate for any member of the group to use this mail account for personal business or other business beyond the original scope: any infringement of the conditions of issue of such a mail 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 sponsors of the account), a mail 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 a mail account for the transmission of agreed local business of one such trade union. In all cases, the granting of any mail 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 a mail 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 a mail 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.

There is no medium of access designated as primary medium for this class of accounts. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

### **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 a mail account for the purpose of transacting specified business of the local branch on behalf of its members. Such a mail account will be issued for a fixed period, and there will be no rights of access to the mail account following its termination (whether at the end of the fixed period or following rescission at an earlier date).

It is inappropriate for such a mail account to be used for purposes other than those agreed by the Director of the Computer Centre, 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 mail account privileges in the manner laid out for a new account under this heading.

The Director of the Computer Centre will have the discretion to allow or deny the hosting upon the Brunel University Data Network of any mailing list on behalf of any Brunel-recognised trade union, and to place any restrictions upon the membership of the list, the ability to manage the list, and the use to which the list may be put.

### **4.4.2 Brunel staff as officer at another level of a Brunel-recognised trade union**

There is no entitlement to a mail 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 a mail 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 a mail 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, in association with access to the Brunel University Data Network, have a mail account, in order to undertake specific internal communication within Brunel. 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.

There is no medium of access designated as primary medium for this class of accounts. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

### **4.5.1 Contract academic staff**

A member of staff from another academic institution contracted to undertake work for the University may, at the discretion of the Director of the Computer Centre and following consultation with the appropriate Head of School, be granted a mail account for the purpose of internal communication within Brunel. For reasons of compliance and records management, the use of such a mail account for personal business, or any other business not connected with the contracted tasks, is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

### **4.5.2 Contractor company staff**

A member of staff of a company contracted to undertake work for the University may, at the discretion of the Director of the Computer Centre and following consultation with the appropriate Head of School, be granted a mail account for the purpose of internal communication within Brunel. For reasons of compliance and records management, the use of such a mail account for personal business, or any other business not connected with the contracted tasks, is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

### **4.5.3 Supplier support staff**

A member of support staff of a supplier company of the University may, at the discretion of the Director of the Computer Centre and following consultation with the appropriate Head of School, be granted a mail account for the purpose of internal communication within Brunel. For reasons of compliance and records management, the use of such a mail account for personal business, or any other business not connected with the contracted tasks, is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

### **4.5.4 Field testing**

At the discretion of the Director of the Computer Centre, a mail 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. For reasons of compliance and records management, the use of such a mail account for personal business, or any other business not connected with the field testing, is inappropriate. At the end of this time period, there will be no access to the account. 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 mail access, in association with a network account issued in order to facilitate Council business under the sponsorship of the Secretary and Registrar of the University. For reasons of compliance and records management, the use of such a mail account for personal business, or any other business not connected with Council membership, is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

There is no medium of access designated as primary medium for this class of accounts. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

## 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.

There is no medium of access designated as primary medium for this class of accounts. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

### 4.7.1 *Professor Emeritus*

A Professor Emeritus of Brunel University is entitled to a mail account for the purposes of maintaining academic communication with Brunel University, under the sponsorship of the Secretary and Registrar of the University. For reasons of compliance and records management, the use of such a mail account for personal business is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

### 4.7.2 *Fellow of the University*

A Fellow of Brunel University is entitled to a mail account for the purposes of maintaining academic communication with Brunel University, under the sponsorship of the Secretary and Registrar of the University. For reasons of compliance and records management, the use of such a mail account for personal business is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

### 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 a mail account for purposes relevant to the association. For reasons of compliance and records management, the use of such a mail account for personal business is inappropriate. There will be no right of access by the account-holder following the mail account's 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 a mail account with characteristics appropriate to such status. There will be no right of access by the account-holder following the mail account's 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 a mail account with characteristics appropriate to such status. There will be no right of access by the account-holder following the mail account's 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 a mail account at Brunel University.

### **4.7.7 Academic collaborator**

At the discretion of the Director of the Computer Centre, an academic collaborator may be granted a mail account to facilitate communication within the collaborative group. For reasons of compliance and records management, the use of such a mail account for personal business is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

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

At the discretion of the Director of the Computer Centre, a collaborator from a non-academic third party may be granted a mail account to facilitate communication within the collaborative group. For reasons of compliance and records management, the use of such a mail account for personal business is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

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

A member of staff of a company associated with Brunel University<sup>9</sup> may be granted a mail account in association with a network account so granted. For reasons of compliance and records management, the use of such a mail account for personal business is inappropriate. There will be no right of access by the account-holder following the mail account's termination.

## **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.

There is no medium of access designated as primary medium for this class of accounts. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

### **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 a mail account at Brunel University for an agreed fixed period. There will be no right of access by the account-holder following the mail account's termination.

---

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

---

### **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 a mail account at Brunel: access to home mail (only for members of the worldwide academic community attending an academic conference organised by a member of the academic staff of Brunel University) may be effected through network account facilities to the conference as agreed at the discretion of the Director of the Computer Centre after any petition by the member of Brunel staff organising the conference.

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

There is no entitlement to a mail account at Brunel University for a student of another institution.

## **4.9 External account-holder**

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

There is no medium of access designated as primary medium for this class of accounts. The format of any electronic mail address or alias will be as decided by the Computer Centre, and there will be no general right of divergence from the address as assigned by the Computer Centre. In particular potential name-clashes may restrict options for such addresses and aliases.

### **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 have mail access as a Brunel user. The Director of the Computer Centre will cooperate 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**

There is no entitlement to a mail account for a general external person.

## **5 Transacting Brunel business by electronic mail**

The transaction of Brunel business by electronic mail is official, and the messages so transacted become official records of the University. They are thus subject to the University’s rules on records management and (where applicable) on data protection and freedom of information. For this reason, all Brunel academic or corporate business will be transacted, by student or staff member alike, using the official Brunel mail account issued for the purpose.

A message sent from a non-Brunel mail account<sup>11</sup> shall be treated as an external message, and will not be acknowledged as carrying official Brunel business. The tampering with the header fields in a message sent from such an external source in order to impersonate an internal Brunel message or to suggest its having come from a Brunel mail account is considered to be tantamount to mail-forging and is therefore considered an unacceptable use of the Brunel mail account.

---

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

<sup>11</sup> such as a staff member’s private ISP mail account

## 6 Acceptable use

The University provides electronic mail and ICTS facilities 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 any level which might impinge on the free flow of University mail for primary-purpose use
- the transmission of unsolicited commercial, advertising or petitioning material (including any such mail in conjunction with charitable organisations or purposes), chain letters or other junk mail of any kind.
- the unauthorised transmission to a third party of confidential material concerning the activities of the University.
- the transmission of material which, by its transmission, infringes the intellectual property rights (including, but not confined to, copyright and patent protection) of another person.
- the creation, transmission and/or storage of any offensive, obscene or indecent images, data or other material unless by an individual registered as having a requirement as part of their work or research to transmit or receive 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 a mail account held on, or accessed via, the Brunel University Data Network. In particular, users should note that connection to a Brunel mail account by link from beyond the Brunel University Data Network imposes the same responsibilities upon the account-holder, including all compliance and records-management responsibilities, and are reminded to satisfy themselves, before attempting to make use of a host's connection, of that host's compliance with the University's requirements on disclosure, retention and disposal.

## 7 Ownership, custody, agency and disclosure

### 7.1 Ownership

All electronic mail created and maintained on Brunel University's electronic mail systems is the sole property of Brunel University. The University deploys countermeasures against the infiltration of its systems by unsolicited bulk and commercial electronic mail, viruses, worms and other vexatious entities. Messages which, by nature of content, subject title, headers or other attributes are deemed to exhibit sufficiently high probabilities of being vexatious may be logged, tagged, quarantined, dropped or otherwise managed in order to minimise the risk of disruption to mail and other ICTS facilities of the University, and/or in order to safeguard the university's reputational integrity.

### 7.2 Official record of the University

An electronic mail message that contributes to the academic or corporate business of the University is an official university record. For this reason, such business must always be transacted using the official mail account(s) provided by the University for the purpose (*i.e.*, the appropriate mail account of the form **mailname@brunel.ac.uk**). The message, once transacted, becomes subject to University policies regarding records management. In particular, any message to or from a staff account becomes archivable into the Brunel Central

---

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

Archive. It is the duty of the member of staff (whether sender or recipient) to archive by proactive means any message which may have evidential importance, even before its automatic ingestion into BCA.

### 7.3 Personal use of the mail account

The University encourages the use of electronic mail as a primary medium of communication, and allows its mail accounts to be used for personal purposes, as long as such use

- is made using a mail account which is entirely personalised to the individual concerned, and which is not characterised as inappropriate for personal business use
- is reasonable, is not disproportionate to primary-purpose use, nor is in any way detrimental to the system's availability for primary-purpose use
- is not for commercial or profit-seeking purpose, nor in furtherance of any financial gain to the sender or (by the agency of the sender's solicitation) to any third party<sup>13</sup>
- 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

Furthermore, it is the duty of each account-holder to ensure the clear separation, within a Brunel mail account, of personal mail business from University business through clear and hierarchical folder management, and to prefer at all times the use of privately-held mail accounts over a Brunel account for the transaction of personal business. The use of a Brunel network account to access such a privately-held mail account is regulated by the characteristics of that network account<sup>14</sup>. The University will not make any alteration to configurations of countermeasures in order to facilitate delivery and/or transmission of personal or other mail which is not primary-purpose. The University will not be held liable for any loss or damage consequent upon, or connected with, any use of a Brunel mail account for personal purposes.

### 7.4 Monitoring mail

The University has a right to inspect, monitor or disclose electronic mail passing through its 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 mail
- there has been 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>15</sup>.

---

<sup>13</sup> including, it should be noted, any individual, not-for-profit or charitable entity as well as a commercial third party

<sup>14</sup> see the University's network account policy

<sup>15</sup> See, for example, <http://www.archive.official-documents.co.uk/document/parlment/nolan/nolan.htm>

## 7.5 Custody of messages

Responsibility for the custody of a message held within the Brunel mail system rests with the account-holder in whose mailbox the message is stored. This responsibility applies along the entire lifecycle of the message. Account-holders should note that such responsibility extends to all folders within the mailbox, including folders containing sent messages.

## 7.6 Custody by agency

The appointment of an agent (or of several agents working individually or collectively) with partial or total access privileges to the mail account of another does not change the responsibility for any action. The account-holder remains responsible for all data stored, transmitted or otherwise subjected to user action within the mailbox associated with the account, and the agent who creates, edits, transmits, deletes or otherwise acts upon data within the account-holder's mailbox 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.

## 7.7 Disclosure

A message 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.

In addition, normal operation of the mail service may, in the context of a technical investigation or simple account management, result in "accidental disclosure" within the investigative or operational team: see also the subsections below on technical investigation (within sections discussing delegated access). Note also the section on *Professional immunity* below.

### 7.7.1 Disclosure of a business message

First and foremost, it should be noted that all messages within a mail account are deemed to be 'business messages' unless clearly labelled as personal and stored accordingly. Messages which are clearly labelled as personal, and which are stored accordingly and adequately separately from other messages, 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 a business message 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 mailbox) in the Head of School (or analogous unit of the University).

### 7.7.2 Disclosure of a message identified as personal

The identification of a message 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 message to be treated immediately as a business message.

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

- the appropriate Head of School, in the case of disclosure from a Brunel student mail 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 mail account other than a Brunel student mail account (as defined above)

## 8 Principles of access

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

- access to a Brunel mail account by the account-holder and others
- access to a mailbox within a Brunel mail account by the account-holder and others.

These are covered in subsections below.

### 8.1 Access to a mail account

An account-holder's primary mode of access to a mail 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 mail system lies wholly within the University. Access may be made to a mail 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 mail 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 mail account.

Access to a mail 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.

### 8.2 Access to a mailbox

Once access has been gained to a Brunel mail account, an account-holder has access to such mailboxes 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 a mailbox 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 a mailbox if mail-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 mailbox 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 mail 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 mailbox, and of the owner of the mailbox to ensure that each permitted accessor is aware of the responsibilities associated with the granting of mailbox access and with the possibility of access restriction.

## 9 Delegation of access by the account-holder

Under certain conditions, full or partial access to a mailbox, or to a restricted set of folders within a mailbox, may be delegated by the account-holder to the holder of another mail 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 mail account. The agent also bears responsibility for compliance with all relevant policies, rules and legislation in carrying out any action on the delegator's mail 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 expressly 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 of access, a change to an existing delegation of access, or the withdrawal of delegate access, to a mail account.

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.

Users should note that, within a corporate messaging system<sup>16</sup>, mail is interwoven with calendar management, task management and other features, and that delegation of, for example, calendar management will engender electronic mail which will need to be managed by the delegate. For this reason, the delegation of any tasks within a corporate messaging system will fall within the meaning of “mail account delegation”.

## 9.1 Agent

Perhaps the most well-known instance of delegation within a mail 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<sup>17</sup>, and this message should be retained and managed according to the standard procedures for task-related direction (including immediate and proactive deposition into the Brunel Central Archive) — 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.

## 9.2 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). Given the likely similarity of actions between a principal and a deputy, a deputy communicating with delegate powers to a principal's mailbox should always make it abundantly clear whether the delegate powers being applied are of communication or of action.

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 (including immediate and proactive deposition into the Brunel Central Archive) — 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.

## 9.3 Group member

There are many instances within the University of mail being sent simultaneously (preferably via a post-based mailing list) to all members of a peer group<sup>18</sup>. In the management of such mail, the group members must always ensure that they act on behalf of the group. First and foremost, a group member should make all effort to keep the

---

<sup>16</sup> *e.g.*, Microsoft Outlook

<sup>17</sup> this will often be generated automatically by the software

<sup>18</sup> such as **computing** support

electronic conversation at group level where appropriate: any privatisation (to a dialogue between group member and customer) must be agreed with the group and (wherever possible) with the customer beforehand. The minimum level of effort for this purpose will be the ensuring that the Reply-to field is always set to the group address, and that the signature bears the imprimatur of the group, and not of the individual.

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 (including immediate and proactive deposition into the Brunel Central Archive) — 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.

## 9.4 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 (including immediate and proactive deposition into the Brunel Central Archive) — 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.

## 9.5 Technical investigation

A user may, through a service enquiry, request a technical investigation which must result in access to that user's mailbox: this will be considered delegate access with the consent of the account-holder.

### 9.5.1 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 by any one of the above investigative authorities, who must make any relevant declaration of interest before proceeding.

---

## 9.5.2 Accidental disclosure

During the course of a technical investigation into the mail service, there may occur the need for a message 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.

## 10 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 mailbox for the account. In this case, the Computer Centre must act in conjunction with the relevant senior managers of the University<sup>19</sup> and with the appropriate Head(s) of School(s).

### 10.1 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 a mailbox, 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 mailbox. The Director of Human Resources may act for and on behalf of any Head of School.

### 10.2 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>19</sup> usually the Director of Human Resources in the case of a staff mailbox, or the Registrar in the case of a student mailbox: both of these managers may be involved in the case of staff access to a student mailbox

---

## 10.3 Internal disciplinary process

Messages held within the Brunel mail system 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*).

### 10.3.1 Staff

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

### 10.3.2 Student (academic discipline)

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

### 10.3.3 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.

## 10.4 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 mail accounts, the need to maintain the smooth operation of mailflow 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.

### 10.4.1 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 Director of Resources and Operations
- the Director of Human Resources
- the Director of the Computer Centre

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

### 10.4.2 Accidental disclosure

During the course of a technical investigation into the mail service, there may occur the need for a message 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.

## 10.5 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 electronic mail accounts, the need to maintain the smooth operation of mailflow 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.

## 11 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 messages and their contents as it sees fit. Great care will be taken in such management to avoid the inadvertent loss of genuine mail which advances the business of the University, but it is recognised that automatic filtering, however efficient, remains an inexact science. In common with all reasonable users of electronic mail, a Brunel user will be happy to re-send a genuine business message which has been lost to the recipient through the *bona fide* application of management rules, making any reasonable amendment to text and/or header to avoid a similar loss of the re-sent message: any Brunel user thus affected should ask the sender to follow a similar procedure.

### 11.1 Countermeasures against vexatious mail

The University will deploy countermeasures against the attempted infiltration of the Brunel mail system and its users' mailboxes by vexatious mail<sup>20</sup> from whatever source or apparent source. In the application of such countermeasures, an incoming message may be subject to one or more aspects of management, including (but not limited to)

- the logging of header details, and of any management trigger (*e.g.*, the incidence of a particular word or phrase in the text of the message or any attachment)

---

<sup>20</sup> spam, viruses, or other mail which impinges on the free flow of primary-purpose mail

- 
- the insertion of information relevant to the countermeasure management (such as a spam-likelihood score) into the message header
  - the quarantining of the message
  - the removal of any attachment from the message which is deemed to raise a risk of vexatious infiltration
  - the deletion of the message from the Brunel mail system

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 a message.

The countermeasures deployed by the University may include the searching for personation, whereby header fields may be altered to disguise the source of the message by suggesting a false source. Such countermeasures will inevitably trap any attempt by a Brunel user to suggest that mail from another source<sup>21</sup> is in fact from within Brunel: since this is unacceptable use of a mail account, the Computer Centre will not relax its defences to accommodate such personation (or mail-forging), and may apply sanctions and/or invoke disciplinary proceedings as deemed appropriate.

## 11.2 HTML filtering

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

- delivery management based upon elements of HTML code within the message
- 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 seek to allow the free flow of primary-purpose content while protecting against vexatious content, adjudicating based on the balance of risk.

## 11.3 Disclaimer

The University reserves the right to attach an appropriate disclaimer or similar text to any message sent from within the Brunel mail system, and to require that no such text is removed or amended during the sending process.

## 11.4 Header data

Each message contains header data to aid message management throughout the transaction process: these data may be

- edited at Brunel as part of its message management
- used by the University for the purposes of auditing, system improvement, or mailflow investigation

The tampering with header data by any user for the purposes of personation, deception or other action unnecessary for the free flow of primary-purpose mail is deemed to be unacceptable use of a mail account.

---

<sup>21</sup> for example, a home ISP mail account

## 11.5 Industry-standard and best-practice procedures

The University does not exist in an electronic-mail vacuum, untouched by others. Mail practices and procedures are re-established with every change or upgrade to a mail client, and evolve as understanding grows of good practice or, conversely, of threats and risks take advantage of loopholes which become bad practice. The University is keen to maintain its reputation as a responsible mail-source, 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.

## 12 Professional immunity

In the course of maintaining the Brunel mail system, 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 such technical infractions committed as a necessary part of such work.

## 13 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 mail 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 mail system 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.

## 14 Security

Confidentiality of electronic mail cannot be guaranteed. It is the responsibility of each member of staff to exercise their judgment when dealing with sensitive issues — extreme caution should be taken when using electronic communication to transmit confidential or sensitive matter (*e.g.*, personal information relating to health, disability and criminal record).

Backup and archive 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. These files are deemed to be discoverable under relevant legislation in the same way as the original messages.

In terms of formal security gradings of UK government data, the BUDN and its attendant systems (including the Brunel mail system) have not been declared qualified to store or manage data classified at a security grading higher than *Restricted*.

## 15 Data protection

Any electronic message which resides on the Brunel University Data Network and which contains personal information (as defined by the Data Protection Act 1998) comes within the scope of that Act, and therefore may be disclosed on request to the subject of that information.

Electronic mail which, in accordance with good record-keeping practice, has been deleted from mail-system storage (and, where relevant, from storage within the Brunel Central Archive) before a request is received under such auspices as Data Protection and Freedom of Information legislation may not, in the context of such a request, be retrievable from backup files held for the purposes of system-wide disaster recovery and business continuity, owing to the unstructured nature of such backup storage.

## 16 Responsibility

### 16.1 Responsibility of individual users

Each user is responsible and accountable for the electronic mail sent from any mail account issued to that user or for the use of that user.

Each user of electronic mail at Brunel has a duty of care to

- ensure that appropriate and proper electronic mail use and management is practised at all times
- understand all personal and group responsibilities with regard to electronic mail use and management
- maintain current awareness of policies, practices, threats and problems relating to electronic mail at (and where relevant, beyond) Brunel
- maintain up-to-date knowledge of Brunel's e-mail client software as it evolves, and take full advantage of its facilities to aid the use, management, storage and retrieval of messages

The Head of each School (or equivalent group within the University) is responsible for ensuring that each member of School staff is aware of this electronic mail policy and that each abides by it at all times.

Each student must realise that enrolment at the University imposes a duty to follow the University's electronic mail policy at all times when using a Brunel mail account, and imposes a responsibility to check that mail account for University mail on a regular and timely basis (including checking at appropriate intervals when off-campus).

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 electronic mail use.

### 16.2 Responsibility of managers

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

---

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 messages within the mailbox(es) of staff or students within his/her School (or similar).

In sensitive cases, the Head of School (or equivalent) should refer matters regarding access to student mailboxes 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 mail.

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 mail.

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.

## **17 Disciplinary procedure**

In the event of an apparent breach of the Brunel Acceptable Computer Use Policy, of this Policy, or of a related Policy by a user or group of users, the Director of the Computer Centre, or his designated agent, has the authority to withdraw access to the facilities summarily 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.