Information Strategy

Electronic mail policy

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

July 2015

Document properties

Authority

Director, Computer Centre

Sponsor

Director, Computer Centre

Responsible officer

Assistant Director (Governance and Corporate Services), Computer Centre

Recent version history

Current version, August 2014, is derived from and supersedes version published in February 2014 and earlier versions.

1 Introduction

1.1 Nomenclature

Hereinafter, where such usage is unambiguous, we may refer to key entities in concise form. These include

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

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

1.2 Scope

Brunel University London must clarify how electronic mail should be used and managed by everyone within the University, as there is a common misconception that electronic mail messages are by nature entirely informal and/or ephemeral. At Brunel University London, electronic mail is recognised as a formal communication medium for the transaction of Brunel University London business, 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). Electronic mail which passes through accounts provided by the University but managed on behalf of Brunel University London by a third party is deemed to fall within the scope of this Policy with the same underpinning principles as for locally-managed mail.

This Policy sets out the accepted use and management of Brunel University London'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 Brunel University London is compliant with all relevant legislation, and that it adheres to the Seven Principles of Public Life in the United Kingdom (popularly known as the Nolan Principles)[1] and to high standards of ethical value, in its management of network computer accounts.

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

2 Supervening policies and frameworks

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

2.1 Brunel Acceptable Computer Use Policy (BACUP)

All computer use which takes place on, or routes activity through, the Brunel University London data network, or through accounts provided by the University for the transaction of Brunel University London business but managed on behalf of Brunel University London by a third party, is subject to the provisions of the Brunel Acceptable Computer Use Policy (BACUP).

The current text of BACUP may be found, co-located with other relevant policies and documents, at **http://www.brunel.ac.uk/life/study/computer-centre/policies/** and is also contained within the Student Handbook. This forms part of Brunel University London's rules.

2.2 Joint Academic Network (JANET)

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

The Counter-terrorism and Security Act 2015 places duties upon the University, including monitoring, alerting and evidence-gathering procedures, to prevent the spread of terrorism and the drawing of people into terrorism. In addition to the countermeasures applied to electronic mail in general, these

2 See **http://www.ja.net/documents/publications/policy/aup.pdf**

duties may involve investigation of the mail component of activity which is not *prima facie* ICTS-related. The Brunel Acceptable Computer Use Policy (BACUP) outlines duties related to this and other relevant legislative instruments.

2.4 Supranational jurisdictions

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

2.5 Ethical soundness of practice

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

3 Components of 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 Brunel University London's electronic mail service.

3.1 Brunel University London electronic mail account

A *Brunel University London electronic mail account* (within this Policy called a *mail account*) is, as appropriate, either a subsidiary service account within the parameters of the account-holder's *Brunel University London network computer account*, or is an account provided by Brunel University London to be operated on a facility managed on behalf of Brunel University London by a third party.

It is the means by which a registered Brunel University London user may carry out Brunel University London's business by electronic mail within the parameters set by the Brunel Acceptable Computer Use Policy (BACUP), by other relevant Policies, Rules and Regulations of Brunel University London, and by supervening laws. Indeed, this mail account is the only official means of communicating Brunel University London business, whereby these business messages become official records of the University. It is therefore critically important that staff and students use their Brunel University London 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 University London 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 Brunel University London 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[3] 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** or ***mailname*@my.brunel.ac.uk** (it is entirely case-insensitive), depending on the system hosting the account.

In certain cases, a 'text equivalent' version of the account-holder's name will be made visible to correspondents: this data field is populated from the relevant data in the student records database and the Human Resources database for student and staff accounts respectively.

3.2 Post-holder aliases and mail-lists

Much of Brunel University London'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 and publish 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 University London 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[4]. 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 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.

---

3 normally the user's name in the format *firstname.lastname*

4 through strict use of the group mail-list in the *To* and *Reply-to* fields when sending and replying respectively

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 University London's mail system

When we refer to *Brunel University London's mail system*, we mean the servers and software located in Brunel University London and elsewhere which contribute to the delivery, flow, accessibility and storage of mail, and to the services which contribute to the ability to carry out Brunel University London's mail business from elsewhere.

This includes the Brunel Central Archive (BCA) of messages sent to or from a staff electronic mail account, and electronic mail facilities managed on behalf of Brunel University London by third parties.

3.4 External and internal mail

Mail which operates wholly within the Brunel University London mail system is considered to be internal mail. The accessibility of the Brunel University London mail system from beyond campus boundaries makes the definition of internal mail independent of geography.

For example, a message sent from one Brunel University London mail account to another using Brunel University London's *Outlook Web Access* service is considered to be internal mail. Conversely, a message sent from or to an account managed and operated independently of Brunel University London, 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 Brunel University London mail account may be accessed through that account's *mailbox* via a communicative medium approved for the purpose by Brunel University London: 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 University London 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[5].

3.5.3 Archive

While a message is in a mailbox, it is immediately available for use by the account-holder[6]. At a later stage, the message within the central mail system hosted at Brunel University London may be removed from the mailbox, to be made accessible from the Brunel Central Archive (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. The archival of messages held in facilities managed by third parties on behalf of Brunel University London will follow norms local to the hosting facility as published by the management of the relevant facility.

It is important to note that the act of archiving a message forms part of the management of that message, and therefore falls within Brunel University London's Records Management policies.

Furthermore, a user may decide to move or copy a message into a file which resides beyond the reach of Brunel University London'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 Brunel University London's Records Management policies will continue to apply.

3.6 Message types

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

- an **official message** of Brunel University London is a message passed from one post-holder to another, or to a group of post-holders: it transacts Brunel University London business which arises by virtue of the posts held (*e.g.*, from the Safety Officer to senior officers of units of the University, or from the account manager of a supplier company to a departmental administrator), irrespective of the identity of the individual incumbents.

---

5 a message sent to multiple addressees at Brunel University London 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

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

- an **administrative message** of Brunel University London is a message which transacts Brunel University London business between an individual and a post-holder at the University, or which passes Brunel University London business between an individual and a post-holder for appropriate consideration and execution. The crucial difference from an official message is that the individual is acting *as an individual*, irrespective of role — for example, a message sent by a member of staff to an administrator enquiring about current holiday entitlement is an administrative message.
- an **individualised message** transacts Brunel University London 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 University London is to process messages which further the academic or corporate business of Brunel University London. This is known as the *primary purpose* of the Brunel University London 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 Brunel University London mail account is subsidiary to the entitlement to a Brunel University London network computer account, policy for which is described in Brunel University London'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.

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.

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

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

4.1 Brunel University of London's staff

A member of Brunel University London's staff will generally be issued with a mail account for the duration of a contract of employment or of an analogous agreement, as part of the service accruing to a general network account. The authority for conferring current Brunel University London staff status rests with the Director of Human Resources[7].

The primary medium of access for such an account will be Brunel University London'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 London.
- 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 London data network.
- The PC has been configured with the image approved by the Computer Centre for use to access the Brunel University London 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 London data network or to use any service associated with the use of Brunel University London'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 Brunel University London 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.

---

7 or, as agreed, through a competent and duly appointed agent

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 Senior Officer of the relevant unit of 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 London 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.

It is the responsibility of the account-holder and of the Senior Officer of the relevant unit of 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 London 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 Senior Officer of the relevant unit of 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 London data network on that date. Such discussions should take place at least two months before the termination date. The issue of a Brunel University London mail account to a temporary member of staff will require that the Senior Officer of the relevant unit of 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 Brunel University London by an external person volunteering service (for example, an alumnus giving time for a 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 termination of the network account.

It is the responsibility of the account-holder and of the Senior Officer of the relevant unit of 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 London 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 Senior Officer of the relevant unit of 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 London 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 London is not appropriate.

4.1.6 Non-retired former staff member

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

4.1.7 Field testing

The granting of a mail account in association with any Brunel University London 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 London, then a mail account will be issued to that person in the capacity of a student on the appropriate course, which will run concurrently with the staff member's role-related account 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 Brunel University London *in loco studentis* will be considered to have account access as a delegate for the student concerned (see appropriate sections under *Brunel University London student*). Any mail account needed for administrative contact between the support worker *per se* and Brunel University London 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 and Dyslexia Service.

4.2 Brunel University London student

A student duly registered on a course of study at Brunel University London 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 Senior Officer of the relevant unit of the University. This account may reside on a facility which is managed by a third party on behalf of the University, with authorisation provided by the University with access privileges commensurate with specific student status.

In any instance of a student's progression from one course of study at Brunel University London to another, there will be no entitlement of 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 Brunel University London'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 London.
- The PC is owned and managed by the Computer Centre as a standard-type PC for the purposes of accessing the Brunel University London data network.
- The PC has been configured with the image approved by the Computer Centre for use to access the Brunel University London 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 London data network or to use any service

associated with the use of Brunel University London's standard mail client in the standard manner.

An attempt to use any other mode of access may encounter access restrictions or diminution of facility. The format of any electronic mail address, alias or associated display data will be as decided by the Computer Centre, and there will be no general right of divergence from the address format 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 London, 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 London, 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 London, 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 London, 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 London, 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 London, 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 London, 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 London, 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 London, or to any other status at Brunel University London, 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 the Policies of Brunel University London during the period of registration for the course of study for which the account is issued, except during any period of suspension of access imposed for any reason as laid out in the Regulations and Policies of Brunel University London.

4.2.7 Part-time student

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

4.2.8 Continuous professional development

A student who undertakes modular study at Brunel University London within a programme of continuous professional development (or similar structure) may, at the discretion of the Director of the Computer Centre and following consultation with the Senior Officer of the relevant unit of the University, be granted 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 London, or otherwise to another status within Brunel University London, 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 the Policies of Brunel University London during any period of Work Placement as an integral part of the course of study for which the account is issued, except during any period of suspension of access imposed for any reason as laid out in the Regulations and Policies of Brunel University London. Rights of connection to the Brunel University London data network, or of access to data held therein or elsewhere, from a connection-point which is not owned or managed by Brunel University London[8], fall entirely within the discretionary powers of the owner or manager of that connection point. See also *Student undertaking work for Brunel University London*.

4.2.10 Former student

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

Agreements with third-party providers of facilities on behalf of Brunel University London may differ, with the possibility of some provision (whether temporary or permanent) after graduation. Any such access will be granted within the terms of agreement between the Computer Centre and the relevant third party.

It is fundamentally important to remember that the provisions and conditions of this Policy, the Brunel Acceptable Computer Use Policy, and other relevant Policies of Brunel University London still apply to use of an account granted by Brunel University London (whether that account is hosted within Brunel University London or by a third party on behalf of Brunel University London), and that sanctions for infraction of these Policies are still retained by Brunel University London, to the extent that access may be restricted, suspended, or withdrawn summarily by Brunel University London.

4.2.11 Student undertaking work for Brunel University London

If, during a course of study, a student undertakes work (whether or not for reward) for Brunel University London, a mail account may, at the discretion of the Director of the Computer Centre and following consultation with the Senior Officer of the relevant unit of the University, be issued with a status appropriate to the work being undertaken[9], 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

8 for example, from the workplace during placement

9 this will normally be as a Brunel member of staff

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 Brunel University London by a student of Brunel University London. See also the section(s) appropriate to the work role.

4.2.12 Distance learner

A student enrolled upon a course of study by distance learning which is provided by Brunel University London is entitled to 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 Brunel University London, gain delegate access *in loco studentis* to the student's Brunel University London mail account. The support worker's own correspondence with Brunel University London should be carried out using an appropriate staff mail account (see appropriate sections under *Brunel University London's staff*.

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

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

Brunel University of London's 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 with Brunel University London 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 Brunel University London. The characteristics of the account may differ from those of an account issued to an analogous member of staff of Brunel University London, for compliance and other reasons.

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 Brunel University London. 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 University London

Brunel University London recognises certain trades unions as representative bodies for groups of staff within Brunel University London. Though these are third-party organisations (and therefore do not fall within much of the licensing structure of Brunel University London's software portfolio), there may be

occasions when it is mutually beneficial to grant access to 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 Brunel University London.

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 London data network in connection with the use of such a mail account constitute records of Brunel University London, and must be managed as such. Responsibility for custody and content lies with the appropriate trade union: this, does not prevent Brunel University London from taking action (including disciplinary action) in the event of inappropriate usage of such an account.

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 Local officer of a union recognised at Brunel University London

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 University London branch of a trade union duly recognised at Brunel University London, 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 London data network of any mailing list on behalf of any trade union recognised at Brunel University London, 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 Elected officer of a union at a non-local level

There is no entitlement to a mail account for the transaction of business of a trade union duly recognised at Brunel University London for any member of staff of Brunel University London who holds an office in a trade union duly recognised at Brunel University London where the duties associated with that office

extend beyond activity carried out on behalf of its members employed by Brunel University London. Furthermore, it is inappropriate for such business to be transacted using the staff member's primary Brunel University London mail account.

4.4.3 External officers of a union

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

4.4.4 Trades unions not recognised at Brunel University London

There is no entitlement to a mail account for the transaction of business of a trade union not recognised as a representative union at Brunel University London. Furthermore, it is inappropriate for such business to be transacted using any other Brunel University London mail account.

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 London data network, have a mail account, in order to undertake specific internal communication within Brunel University London. 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 Brunel University London may, at the discretion of the Director of the Computer Centre and following consultation with the Senior Officer of the relevant unit of the University, be granted a mail account for the purpose of internal communication within Brunel University London. 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 Outsourced services and facilities

A member of staff of a company subject to an outsourcing contract to undertake work for Brunel University London may, at the discretion of the Director of the Computer Centre and following consultation with the senior manager of the University charged with overseeing the outsourcing

contract, be granted a mail account for the purpose of internal communication within Brunel University London. 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 Contractor company staff

A member of staff of a company contracted to undertake work for Brunel University London may, at the discretion of the Director of the Computer Centre and following consultation with the Senior Officer of the relevant unit of the University, be granted a mail account for the purpose of internal communication within Brunel University London. 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 Supplier support staff

A member of support staff of a supplier company of Brunel University London may, at the discretion of the Director of the Computer Centre and following consultation with the Senior Officer of the relevant unit of the University, be granted a mail account for the purpose of internal communication within Brunel University London. 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.

4.5.5 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 Brunel University London for the purposes of field testing. This account will be issued for a fixed period consistent with the requirement for field-testing the particular entity. 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 Brunel University London is entitled to mail access, in association with a network account issued in order to facilitate Council business under the sponsorship of the Secretary to the Council of Brunel University London. 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 Brunel University London, there are several classes of person who may be designated as 'associated' with Brunel University London. 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 London is entitled to a mail account for the purposes of maintaining academic communication with Brunel University London, under the sponsorship of the Secretary to the Council of Brunel University London. 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 Brunel University London

A Fellow of Brunel University London is entitled to a mail account for the purposes of maintaining academic communication with Brunel University London, under the sponsorship of the Secretary to the Council of Brunel University London. 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 institution associated with Brunel University London 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 London 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 — course award validated by Brunel University London

A student of an associated institution who is enrolled on a course of study for an award which is validated by Brunel University London is entitled to 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 — course award validated by student's home institution

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

4.7.7 Academic collaborator

At the discretion of the Director of the Computer Centre, an academic collaborator may be granted a Brunel University London mail account in order to facilitate communication within the collaborative group based at Brunel University London. 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. The attention of the holder of an account of this type is drawn to the requirements to abide by legal and regulatory constraints relating to consumer protection and competition law, as outlined in the Network Account Policy.

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 Brunel University London mail account in order to facilitate communication within the collaborative group based at Brunel University London. 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. The attention of the holder of an account of this type is drawn to the requirements to abide by legal and regulatory constraints relating to consumer protection and competition law, as outlined in the Brunel University London *Network Account Policy*.

4.7.9 Staff of associated company

A member of staff of a company associated with Brunel University London[10] 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.

---

10 for example, a tenant company of the Science Park

4.8 Visitor

The ability of Brunel University London to accommodate visitors' requests for network access is severely limited by the day-to-day pressures on its facilities, and by Brunel University London'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 London for an extended period may, at the discretion of the Director of the Computer Centre, be granted a mail account at Brunel University London for an agreed fixed period. There will be no right of access by the account-holder following the mail account's termination.

4.8.2 Conference delegate

In general, a delegate attending a conference or similarly enjoying the benefits of Brunel University London (for example, a teacher, administrator or student at a summer school located at Brunel University) has no entitlement to a mail account at Brunel University London: 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 London) 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 University London staff organising the conference.

4.8.3 Student of another institution

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

4.9 Audit, review and quality assurance

4.9.1 Audit

A member of an audit company who is visiting Brunel University London to conduct an audit may, at the discretion of the Director of the Computer Centre or the Head of IT Governance, be granted a mail account at Brunel University London for an agreed fixed period. There will be no right of access by the account-holder following the mail account's termination. In the case that an associated network account is re-used, data held within the mail account will be flushed in line with network account data.

4.9.2 Programme review

A member of a programme review board who is visiting Brunel University London to conduct such a review may, at the discretion of the Director of the Computer Centre or the Head of IT Governance, be

granted a mail account at Brunel University London for an agreed fixed period, usually co-terminous with the associated network account. There will be no right of access by the account-holder following the mail account's termination. In the case that an associated network account is re-used, data held within the mail account will be flushed in line with network account data.

4.9.3 Professional accreditation

The accreditative requirements of certain courses with competent professional regulatory bodies may require mail access for the accreditor(s). Access will be granted in line with academic programme review (above), but there may be restrictions placed upon the use of the account consistent with accreditor status.

4.9.4 External examiner and analogous status

An external examiner for academic provision at Brunel University London will be granted a mail account at Brunel University London for an agreed fixed period, usually co-terminous with the associated network account, in order to carry out correspondence within Brunel University London. There will be no right of access by the account-holder following the mail account's termination.

4.9.5 Academic quality assurance

A member of a team visiting Brunel University London to conduct academic quality assurance may, at the discretion of the Director of the Computer Centre or the Head of IT Governance, be granted a mail account at Brunel University London for an agreed fixed period. There will be no right of access by the account-holder following the mail account's termination. In the case that an associated network account is re-used, data held within the mail account will be flushed in line with network account data.

4.9.6 Analogous function

The grant of a mail account for an analogous function will be wholly at the discretion of the Director of the Computer Centre or the Head of IT Governance, with the Secretary to the Council of Brunel University London to deputise in the case of the absence of these two, or in any case of recusation due to a possible conflict of interests: terms and conditions for similar functions will inform decisions.

4.10 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.

4.10.1 General external account-holder

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

5 Brunel University London business mail

The transaction of Brunel University London business by electronic mail is official, and the messages so transacted (including any attachments bound to such messages) become official records of Brunel University London. All of these entities, therefore, fall subject to the rules of Brunel University London pertaining to records management and (where applicable) on data protection and freedom of information. For this reason, all Brunel University London academic or corporate business will be transacted (only and always), by student or staff member alike, using the official Brunel University London mail account issued for the purpose.

A message sent from a mail account which is not managed by Brunel University London[11] shall be treated as an external message, and will not be acknowledged as carrying official Brunel University London business.

The tampering with the header fields in a message sent from such an external source[12] in order to impersonate an internal Brunel University London message, or to suggest its having come from a Brunel University London mail account, is considered to be tantamount to mail-forging and is therefore considered an unacceptable use of the Brunel University London mail account. Any such action may lead to withdrawal or suspension of account privileges and/or disciplinary measures. In serious cases, Brunel University London retains the right to institute legal proceedings and/or to involve the Police.

6 Acceptable use

Brunel University London provides electronic mail and ICTS facilities for use in the furtherance of the learning, teaching, research and approved business activities of Brunel University London: activity which conforms to the above is defined as ‘primary-purpose use’. Brunel University London’s facilities, including such facilities provided by Brunel University London but managed on behalf of the University by a third party, should not be used for

- personal use at any level which might impinge on the free flow of Brunel University London mail for primary-purpose use.
- the transmission of unsolicited commercial, advertising or petitioning material (including any such mail in conjunction with any individual, not-for-profit, political, religious, advocative or charitable entity as well as a commercial third party), chain letters or other junk mail of any kind.

---

11 such as a staff member’s private ISP mail account

12 With the exception of a third party managing a mail facility on behalf of Brunel University London under the terms of an agreement concluded with the Director of the Computer Centre

- any information sharing which may contravene the letter or spirit of consumer protection law as it applies to the assurance of fair competition and fair access across the Higher Education sector in the United Kingdom, the European Union, and elsewhere as relevant.
- the unauthorised transmission to a third party of confidential material concerning the activities of Brunel University London.
- 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, save by an individual registered as having a requirement for work or research to transmit or receive such material.
- the use of any mail facility to promote activity which is the subject of restriction under the Counter-terrorism and Security Act 2015, or to make a connection to an external mail facility in order to promote such activity
- any activity likely to harm the reputation of Brunel University London or the goodwill extended to Brunel University London.

In all cases and at all times, the account-holder is bound by the Brunel Acceptable Computer Use Policy[13] while using any mail account held on, or accessed via, the Brunel University London data network, or provided by Brunel University London but managed on behalf of the University by a third party. In particular, users should note that connection to a Brunel University London mail account by link from beyond the Brunel University London 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 Brunel University London's requirements on disclosure, retention and disposal.

7 Ownership, custody, agency and disclosure

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

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

---

13 available at **http://www.brunel.ac.uk/about/administration/policy/**

7.1 Ownership

All electronic mail created and maintained on Brunel University London's electronic mail systems is the sole property of Brunel University London. 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 Brunel University London, and/or in order to safeguard Brunel University London's reputational integrity.

7.2 Official record of Brunel University London

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

It is the clear and unambiguous 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 the Brunel Central Archive.

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

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

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

7.3 Personal use of the mail account

Brunel University London encourages the appropriate use of technology by its staff and students, and that extends to the use of electronic mail as a primary medium of communication. Brunel University

London therefore allows its mail accounts to be used for limited personal purposes, as long as such use

- is made using a mail account which is entirely personalised to the individual concerned, and 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, nor in furtherance of the dissemination of the aims, ethos, policies, opinions or like matter in respect of any third party, including, it should be noted, any individual, not-for-profit, political, religious, advocative or charitable entity as well as a commercial third party.
- does not conflict with the rules, regulations, policies and procedures of Brunel University London.
- is not of a nature that conflicts with the business of Brunel University London.
- does not promote activity which is the subject of restriction under the Counter-terrorism and Security Act 2015, whether using a Brunel mail account or by making a connection to an external site in order to promote such activity
- is not of a nature which could lead to a diminution of Brunel University London's reputational integrity.

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

7.4 Monitoring mail

Brunel University London has a right to inspect, monitor or disclose electronic mail which passes through its network or through a facility provided by Brunel University London but managed on its behalf by a third party, but will not, as a matter of routine, do so unless

- required by law (including the duties placed upon the University to undertake risk-based monitoring, alerting and evidence-gathering under legislation such as, but not limited to, the Counter-terrorism and Security Act 2015).

- for the purposes of maintaining the free flow of primary-purpose mail.
- there has been a suspected violation of the ordinances, rules, regulations or policies of Brunel University London.

Brunel University London's policies on the inspection, monitoring and disclosure of data are founded upon compliance with all relevant legislation, and with the Seven Principles of Public Life (popularly known as the Nolan Principles)[14], and with Brunel University London's values of fairness, respect and decency.

7.5 Custody of messages

Responsibility for the custody of a message held within the Brunel University London 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 Brunel University London 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 Brunel University London, 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 Brunel University London. Advice will be sought from the Governance, Information and Legal Office of Brunel University London where there is any doubt about the legitimacy of disclosure. In support of the lines of authority for disclosure as laid down below, the Chief Operating Officer and the Vice-Principals have authority to act in the absence of primary authorities, as do, *in extremis*, the Director of the Computer Centre and the Secretary to the Council of Brunel University London.

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

14 See, for example, **http://www.archive.official-documents.co.uk/document/parlment/nolan/nolan.htm**

also the subsections below on technical investigation (within sections discussing delegated access). Note also the section on *Professional immunity* below.

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

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[15], will be observed as such in manual transactions, though automated data transactions will generally be unable to distinguish between the two types of designation. This highlights the clear benefits of rigorous separation of personal and business mail, preferably to the extent of using an external mail account for all mail which is not Brunel University London business.

Authority for the release of a business message to be disclosed to a third party is vested initially in the normal line management of Brunel University London, and alternatively (and directly in the case of disclosure from a student mailbox) in the Senior Officer of the relevant 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 Senior Officer of the relevant academic unit of Brunel University London, in the case of disclosure from a Brunel University London student mail account (*i.e.*, one classified within the subsections of accounts under *Brunel University London student*.
- the Director of Human Resources, in the case of disclosure from any mail account other than a Brunel University London student mail account (as defined above).

15 normally within a separate and clearly identifiable directory substructure

8 Principles of access

It is important to separate out the two strands of the principles of access when dealing with a Brunel University London mail account: these (covered in subsections below) are

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

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

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

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

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

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 University London mail or to the integrity of Brunel University London data or computing services. It is the responsibility of the accessor to ensure that all aspects of this policy and of any other relevant legislation and regulations are observed in any access to a Brunel University London 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. It is furthermore the duty of the accessor to access and use information only in accordance with Brunel University London's values of decency, respect and fairness.

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 London 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 Brunel University London, 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[16], 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".

It is furthermore the duty of the accessor to access and use information only in accordance with Brunel University London's values of decency, respect and fairness. In each instance, every attempt must be made to secure appropriate access to the mail associated with the account without in any way compromising the account-holder's access by changing the access password or any similar means.

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, personal assistant, 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[17], 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

16 *e.g.*, Microsoft Outlook

17 this will often be generated automatically by the software

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

In Brunel University London as in many other organisations, there are many instances of mail being sent simultaneously (preferably via a role-based mailing list) to all members of a peer group[18]. 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 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 group member 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 vital in maintaining an ability to confirm 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 Senior Officer of the principal's unit of the University, the details of delegation may be conveyed to the Computer Centre (via Computing Support in the first instance) if direct delegation is not possible. The scope and duration of delegation should be clearly laid out in a message to the delegate (and, in the case of Computer Centre action, to the principal and to the Senior Officer of the principal's unit of the University, and this message should be retained and managed according to the standard procedures for task-related direction (including immediate and proactive deposition into the Brunel Central Archive) — any subsequent change to this delegation should be similarly managed. This procedure is vital in maintaining an ability to confirm delegated powers in any dispute or investigation.

---

18 such as **computing-support**

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

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

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

The boundaries for such access will be set (and may be changed) in respect of each individual investigator 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 investigation is different, but the following rules apply throughout.

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

Any investigative member of Brunel University London staff who operates beyond the scope of in-force rules with respect to accidental disclosure will be subject to the appropriate disciplinary procedures of Brunel University London.

10 Access beyond 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 Brunel University London[19] and with the Senior Officers of any relevant units of the University. In all cases, it is the duty of anyone granting delegate access to ensure the delegate's compliance with Brunel University London's standards and values of fairness, respect and decency in all use of electronic mail and associated information.

10.1 Business or academic continuity

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

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.

---

19 usually the Director of Human Resources in the case of a staff mailbox, or the Head of Registry in the case of a student mailbox: both may be involved in the case of staff access to a student mailbox

Any information gained by any member of an investigative team is privileged. Any investigative member of Brunel University London staff who operates beyond the scope of in-force rules with respect to accidental disclosure will be subject to the appropriate disciplinary procedures of Brunel University London.

10.3 Internal disciplinary process

Messages held within the Brunel University London 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 Head of Registry.

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 Chief Operating Officer.

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 Chief Operating Officer

- 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 investigative member of staff of Brunel University London who operates beyond the scope of the in-force rules with respect to accidental disclosure will be subject to the appropriate disciplinary procedures of Brunel University London.

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 Brunel University London and its agents to require access without explicit delegation by the account-holder. Furthermore, simple good practice for the purposes of business continuity will require that access permissions are held by competent technical staff. Such access, which will only be invoked in emergency or through technical necessity, is privileged and the

inappropriate disclosure or use of information gained through such accidental access will be handled through normal disciplinary channels and procedures.

See also *Professional immunity* below.

11 Management and filtering

In order to maintain continuity of Brunel University London's academic and corporate business, and in the safeguarding of the University's reputational integrity, Brunel University London 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 Brunel University London, but it is recognised that automatic filtering, however efficient, remains an inexact science. In common with all reasonable users of electronic mail, a Brunel University London 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 University London user thus affected should ask the sender to follow a similar procedure.

11.1 Countermeasures against vexatious mail

Brunel University London will deploy countermeasures against the attempted infiltration of the Brunel University London mail system and its users' mailboxes by vexatious mail[20] 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).
- 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 University London 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.

---

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

The countermeasures deployed by Brunel University London 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 University London user to suggest that mail from another source[21] is in fact from within Brunel University London: 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

Brunel University London 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, Brunel University London 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

Brunel University London reserves the right to attach an appropriate disclaimer or similar text to any message sent from within the Brunel University London 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 University London as part of its message management.
- used by Brunel University London 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. Brunel University London may apply sanctions to the use of any mail account connected with

21 for example, a home ISP mail account

any person under suspicion of such activities, and may pursue such a person through Brunel University London disciplinary process and/or legal procedures as appropriate.

11.5 Industry-standard and best-practice procedures

Brunel University London 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. Brunel University London is keen to maintain its reputation as a responsible mail-source, and will instigate measures to encourage good practice and to inhibit poor practice. In taking such measures, Brunel University London 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 University London 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 Policies of Brunel University London. Users should be aware that, subject to any external restrictions placed upon such activities (*e.g.*, by legislation), staff involved in a *bona fide* investigation or technical operation will enjoy professional immunity against such technical infractions committed as a necessary part of such work.

13 Qualification of access permission

Users should be aware that Brunel University London retains the right to impose qualifications and restrictions on any permission to access a 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 Brunel University London activities.
- in connection with a programme of service maintenance, change or enhancement.
- in response to any information relating to a threat to the security or smooth operation of the Brunel University London mail system or any other Brunel University London service.
- at the discretion of the Director of the Computer Centre for any appropriate cause or reason.

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

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 Brunel University London for the sole purpose of disaster recovery and business continuity on a system-wide basis: they are not regarded as an 'offline repository' in any capacity, nor as a backtracking facility for the restitution of individual files following a reconsideration of the wisdom of any editing or disposal. 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 Brunel University London data network and its attendant systems (including the Brunel University London mail system) have not been declared qualified to store or manage data classified at a security grading higher than *Restricted*.

15 Data protection and retention

Any electronic message which resides on the Brunel University London 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.

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

16 Responsibility

Responsibility for mail account use rests with the individual, and all the way along the management/supervisory chain[22]: for the sake of conciseness, within this section, the term *manager* is to encompass anyone who has a managerial, supervisory or educative relationship with individual account-holders.

Beyond this basic 'internalised' responsibility, it is furthermore the responsibility of each user to encourage high standards of legal, technical and moral compliance in all other users, and to report any lapse from these standards by any Brunel University London user to the Computer Centre, who will assess any need to restrict or suspend access by the offending party.

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 University London has a duty of care

- to ensure that appropriate and proper electronic mail use and management is practised at all times.
- to understand all personal and group responsibilities with regard to electronic mail use and management.
- to maintain current awareness of policies, practices, threats and problems relating to electronic mail at (and where relevant, beyond) Brunel University London.
- to maintain up-to-date knowledge of Brunel University London's preferred messaging software as it evolves, to take full advantage of its facilities to aid the use, management, storage and retrieval of messages, and likewise to take full advantage of other facilities of the said messaging software (in calendaring, task management, etc.), to enhance the efficiency and productivity of Brunel University London in the transaction of its business.

The Senior Officer of each unit of the University is responsible for ensuring that each member of staff within that unit is aware of this electronic mail policy and that each abides by it at all times.

Each student must realise that enrolment at Brunel University London imposes a duty to follow Brunel University London's electronic mail policy at all times when using a Brunel University London mail account, including any account provided by Brunel University London and associated with a facility managed on behalf of Brunel University London by a third party, and imposes a responsibility to check

22 to include tutors and supervisors of students, and the academic management chain above such people

that mail account for Brunel University London mail on a regular and timely basis (including checking at appropriate intervals when off-campus).

The Senior Officer of the relevant academic unit of the University has a duty to ensure that each student within that unit maintains awareness of responsibilities in respect of mail use.

16.2 Responsibility of managers

16.2.1 Managerial responsibility in respect to individual compliance

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

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

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

16.2.2 Managerial responsibility in data access and management

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

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

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

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

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

17 Disciplinary procedure

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

