Brunel UNIVERSITY WEST LONDON

Information Strategy

Electronic mail archive compliance account policy

The purpose of this document is to lay forth the policy which regulates the use of compliance accounts within the University's electronic mail archive. It should be clear that policy is not immutable: in particular, in a field such as this, where emerging technology is interwoven with emerging law, we must be able to react to changes. In the formulation and continuous reformulation of policy, we must be guided by advice from within the University and beyond, taking due consideration of legal precedent, and having due regard to the practices and experiences of our colleagues in other institutions.

Document properties

Authority

Information Strategy Group

Sponsor

Director, Computer Centre

Responsible officer

Policy Development and Quality Manager, Computer Centre

1 Introduction

The University, having resolved to create a searchable archive of electronic mail (known by its proprietary acronym of *IAP*[1]), must clarify how the special 'compliance accounts' should be used and managed within the archive. IAP gives the University (as Data Controller within the meaning of the Data Protection Act 1998) access to electronic mail messages sent to and from members of staff at the University, which are variously archived and journaled. Such access — over and above access by the user to his/her own archive, and for the purpose of legal compliance and/or the maintenance of regulatory obligations — is performed using such specific accounts with special archive-wide privileges, known as 'compliance accounts'.

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

2 Scope of document

This document establishes policy, but co-located with the policy are the procedures which are undertaken to bring assurance of the carrying out of such policy. It is therefore an *operational policy document*.

The corpus of legal compliance and other regulatory obligations are beyond the scope of this document, which seeks only to regulate the use of a compliance account to meet such obligations as are elsewhere defined.

3 Compliance account creation

A compliance account will only be created (or subsequently modified) on the separate authority of **two** of the University's duly nominated Data Officers and on the subsequent confirmation of such authorities by the Director of the Computer Centre (in whose absence, by a deputy nominated by the Director for the especial purpose).

---

1 Integrated Archive Platform — previously known as *RISS*

Each compliance account will be registered to **two** named keyholders, each of whom will be issued with only partial (but complementary) access credentials. This issue (or subsequent re-issue) will be effected to each individual keyholder in turn, in the absence of the other keyholder and under the controlling presence of the IAP Administrator. The sub-password which forms part of each keyholder's credentials will be selected by the keyholder in the presence of, but without disclosure to, the IAP Administrator. The keyholder will neither write down any sub-password nor divulge any sub-password to any other person (including the IAP Administrator),

Each sub-password held by a keyolder will contain at least one upper-case letter, one lower-case letter, and one numeric character within its span. Neither the password nor either sub-password may be changed by either of the keyholders, nor by both working in collusion: any change of password must be effected under the control of the IAP Administrator as for an initial issue of access credentials.

Both keyholders will need to be present at any use of the compliance account. The keyholders will not collude to make known to either or both of their number the complete access credentials for the account.

4 Compliance account use

The use of the compliance account will take place in an appropriate location such that the opportunity for others to overhear or witness transactions is minimised. The Director of the Computer Centre may at his discretion nominate a location for such use. The creation of any hardcopy materials (printout, storage media, etc.) and any subsequent use of these materials prior to their handover to the end user will constitute a use of the account as regards conduct in this section of this policy. Hardcopy will not be directed to be produced on a printer, etc., without both keyholders being present to receive it at the moment of issue.

At all times, both keyholders must be present during any use of the compliance account: if one needs to leave the location of use for any reason and for however shotr a period, the session of use will be concluded and a new session of use commenced at the reconvocation of the two keyholders.

Each keyholder will sign each item of hardcopy as it is issued from the printer, diskholder, or equivalent device.

In the instance of any sequence of data manipulation, one keyholder will annotate a report outlining the steps taken while the other keyholder performs the manipulation.

All hardcopy materials will be kept in a secured location when not in use. Access to the secured location will not be made possible by a single keyholder, through the deposit of the key to the secure area being made with the Director of the Computer Centre or an agent thereof nominated for the purpose.

5 Compliance account audit

Full audit functions must be set to be captured during each session of use of the compliance account. No keyholder will be permitted to manage files pertaining to the audit of a session of use for which he/she was a contributing user. Furthermore, the access of the audit files must themselves be audited, and any use of hardcopy materials must be signed out and signed in on a log-book dedicated to the purpose.

An audit search will be done by the IAP administrator on the last working day of the month the search will find all compliance officer activity for that month. This information will be captured and passed to the Computer Centre Director who will check that each search had 'reason' and was not an 'abuse' of power. Any queries will be raised first with the Data Officers making the search and then, if required, with the Director of Human Resources. These reports must be stored as a record of activity. This information will also be stored in the IAP audit log for a period not less than seven calendar years, nor greater than eight calendar years and one calendar month.

Access to the IAP audit log will only be given to the IAP Administrator and the Computer Centre Director, or to an agent of the Director of the Computer Centre nominated for the purpose.

6 Compliance account demission

At the point at which any compliance account keyholder ceases to be such (whether through departure from the post, through a re-allocation of duties, or for any reason determined by the Director of the Computer Centre, all compliance accounts for which that keyholder acts will be terminated, and fresh accounts initiated with new pairings as necessary.