PROCEDURE FOR ACCESSING PERSONAL ELECTRONIC STORAGE RESOURCES

Table of Contents

1. Introduction

From time to time, the University will require access to personalised storage resources such as mailboxes and personal file stores (H: drive) that are/were allocated to individual members of staff. This typically occurs when a member of staff is ill, has left the employment of the University, or for legal/disciplinary purposes.

It should be noted that while such resources are provided to staff solely for use in relation to their work, there will undoubtedly be some personal information held within them even if only emails from HR or trade unions. Thus, there may be legal implications for the University and its staff in providing such access.

Hence, procedures are required to ensure that the University can continue its business.

2. Avoiding the Situation

While the situation cannot always be avoided, all University departments should take action to minimise the occasions when they may require access to the contents of mailboxes and file stores allocated to individuals. Appropriate use should be made of role based email (e.g. admissions@strath.ac.uk) and I: drive group storage instead of H: drive individual storage. When an employee is leaving the University, their line manager should ensure that they make appropriate arrangements to handover relevant information. When someone leaves the University they should be asked to remove any information personal to them.

3. Permission to Access the Resource

One of the following two procedures must be followed:

If possible and appropriate, the head of department1 (or nominee) of the account holder should contact the account holder to explain the situation, and ask for their assistance. If in agreement the account holder should be requested to provide written authority for an appropriate individual as approved by the University to access the information. Under no circumstances should the account holder be asked for or disclose their login credentials. The written authority should be passed to Information Services (via the Help Desk) who will arrange supervised access to the resource. If appropriate and possible, the account holder would be allowed to be present while the resource was accessed or to arrange to remove personal information prior to the access.

If the member of staff is not contactable, is unable or unwilling to assist, or requesting their assistance is deemed to be inappropriate, a request in writing should be made to the Director of Information Services (or nominee). This request must come from the appropriate head of department. This request should include:

- Details of the resource (i.e. email address, H drive etc)
- For emails details of the time period during which relevant emails may have been received/sent

- An explanation of the circumstances which have necessitated this request

This request must be approved by the Director of Information Services. Guidance may be sought from the Director of Human Resources and other appropriate colleagues. Once approved, Information Services will arrange supervised access to the resource.

In both cases all actions must be fully documented and, while information may be copied, no information may be deleted or amended. When accessing an email account no messages may be sent externally, however obviously business related emails can be forwarded to an account determined by the Head of Department. Any obviously personal information must not be accessed unless relevant to an investigation. On confirmation to the Help Desk of the completion of the appropriate actions access to the accounts will be removed.

1 This includes Deans, Senior Officers and Directors of Services, as well as Heads of Department.