Staff Exit Procedure

Introduction

This document is intended to provide guidance to line managers for the actions required and issues to consider when a member of staff leaves the University.

These arrangements apply to all staff-type accounts, including affiliates, temporary staff and work placements.

Activities can broadly be split into five categories:

Admin Procedures & Forms	Complete paperwork to ensure correct administration on Payroll and HR systems
Planning	To think about the impact that the member of staff's departure will have on departmental operations and plan accordingly
Documents	Important physical documents and files are identified and handed over to a nominated individual.
IT Account – (Data Storage & Email)	Ensure data stored electronically is weeded and retained if appropriate. This includes arrangement for email and the member of staff's IT account
Property	Ensure any University property assigned to the member of staff is recovered

1. Admin Procedures & Forms

1.1 If the member of staff is leaving the university, upon receipt of written notice, a PERS025 Termination form must be completed and passed to the Dean/Head of School/Service before being forwarded to the Personnel Department.

1.2 If available, the original PERS039 form created when the member of staff commenced employment should be obtained from the member of staff's file or a new (revised 2009) form created. The PERS039 form should be used to record the recovery of property and actions relating to access to data (see below). The form is returned to the staff file upon completion and should be held in accordance with data retention policy.

1.3 The remaining leave entitlement for the current leave year should be worked out and arrangements be made for staff to take outstanding annual leave or for leave taken in excess of entitlement to be recovered. Leave details should be added to the PERS025 form.

2. Planning

2.1 A key part of managing any staff absence or departure – be it permanent or temporary – is planning for business continuity. There are many considerations, for example:

- ☐ Who and when to notify?
- ☐ What are the critical duties and responsibilities?
- ☐ Consider references to the individual in web pages, procedures, documentation etc.
- ☐ What is the impact on planned work?
- ☐ What are the priorities for the vacancy?
- ☐ Who will look after these issues in the interim and what additional access rights/resources might they require?
- ☐ Consider representation at meetings and update diaries accordingly.
- ☐ What contingencies are required?
- ☐ Is on–the-job or other training required?

2.2 As soon as possible after notice or notification has been given, the member of staff and line manager should meet to discuss the implications of their departure. It is good practice to draw up an impact analysis and handover plan to address these requirements. This can be shared with other staff, managers and stakeholders to ensure the departure is properly managed.

Planning can and should include access to documents, data and email – these are covered separately and in detail below.

3. Documents

3.1 Arrangements should be made for continuity of access to physical documents or files important to the University. A brief audit should be undertaken, recording the location of important items. Any outdated materials should be disposed of in accordance with the retention schedule. The member of staff should hand over any relevant materials to their colleagues as directed by their line manager.

4. Access to IT Account

4.1 When a member of staff leaves the University, their IT account will need to be terminated.

4.2 After departure, it is the line manager's responsibility to ensure that the account is disabled (see section 4.8). Once disabled, the account will be deleted after 3 months, along with all the data and emails stored. It is therefore vital that the line manager and member of staff make arrangements to preserve access to electronic information important to the business of the University.

4.3 In the event of a sudden or unexpected departure or the member of staff is on long term sick leave immediately prior to leaving, and therefore access is required to information held in the IT account, as a last resort a line

manager may submit a justification and a request for access to the University Secretary, who will consider the request and if appropriate, authorise IT Services to take necessary action.

4.4 It is the responsibility of the member of staff along with the relevant line manager to preserve and retain any data held in the user's account. Information should be stored in accordance with the Information and Records Management Strategy i.e. documents important to the University should be stored in a shared location, controlled by appropriate permissions and accessible by other authorised individuals. Information may also be held on the user's PC, in their Personal Filestore and as emails and attachments stored on the central Exchange server or in a local Outlook file on the PC. There may also be local considerations for data stored on applications, such as academic materials in WOLF or personal information stored in Pebblepad.

4.5 Data

4.5.1 Data stored on the user's PC (usually on the C:\ drive in the "Documents on this PC" directory) should be reviewed by the member of staff and their line manager; archived or copied elsewhere and then deleted. Once the member of staff has left the department, it is good practice to request that IT Services re-image the PC, as this clears it of all data.

4.5.2 Data held in the member of staff's Personal File Store (more commonly known as "My Documents") should be reviewed by the user prior to their departure and any relevant documents passed on to the line manager or appropriate colleagues. This will include any Personal web pages. These data will be lost when the account is eventually deleted.

4.5.3 The line manager should confirm with the member of staff that any confidential or personal data has been removed or destroyed.

4.6 Email

4.6.1 Copies of any important emails and attachments should be sent on to another member of staff prior to departure, by arrangement with the line manager. This includes messages in both the user's Exchange mailbox and in personal folders held in a local Outlook file. The member of staff can copy their email to an archive file that can be copied to CD and left with their line manager if required. Further information can be found on the IT Services Self-Help web pages or alternatively, contact the IT Service Desk for further information.

4.6.2 If the member of staff owns or has administration rights to any Outlook public folders, they should pass these rights on to another member of staff as required.

4.6.3 It is good practice to cancel any mailing list subscriptions and/or to nominate colleagues to subscribe to any that are of interest or importance to the University.

4.6.4 During the notice period, consideration should be given to adding a note on to the member of staff's email signature, alerting people to their impending departure and identifying a contact to use once they have left.

4.6.5 On the day of departure, an out of office message should be set up to inform along similar lines to the message in the signature (see 4.6.4 above), to inform people of the status of the account and to provide alternative information for contacting the University/School/Department.

4.6.6 It may be advisable to arrange for messages to be forwarded to another address. Consideration should be given as to whether a shared public folder/email address may be a more appropriate destination for certain types of email, such as enquiries.

4.7 Specialist Applications

4.7.1 Specific arrangements may be required for the transfer of data held in specialist or local applications, such as academic teaching materials in WOLF or portfolios in Pebblepad. Staff should liaise with colleagues and IT Services as required.

4.7.2 Where an individual uses non-standard software e.g. with a single user licence, consideration should be given to transfer the software to another PC/member of staff if appropriate. Any non-standard software licensed on a named user basis will need to have the license updated.

4.8 Termination

4.8.1 On the day of departure, the line manager must log a call with the IT Service Desk (Ext. 2000) informing them of the departure and ask for the account to be disabled. The call will be passed to the ITS Admin Support team who will disable the account as requested and confirm the action via email to the line manager. This will be copied to administrators of current business systems (Finance, Student Records, HR etc.) for local action as necessary.

4.8.2 Exceptional special circumstances requiring an ex-staff member to have continued access to University IT facilities after they have left should be referred to the Director of IT Services or nominated deputy for consideration. This will require changes to the account to remove its "staff" status. In some cases it may be necessary to create a new external account. There may be an internal quarterly charge for this service.

4.8.3 IT Services will undertake periodic audit checks against the Personnel database. The accounts of staff found to have left without any notification being received from a line manager will be automatically disabled.

4.9 Property

4.9.1 The member of staff may have been issued with University property in support of their current role. Typical items would be a laptop, mobile phone, books, staff ID, keys etc. If the member of staff is leaving the University such items should be recovered near to or on the day of departure.

4.9.2 Issue of these items should have been recorded on a PERS039 form for that individual and stored in their personal file. The form should be used to record recovery of these items.

4.10 Passwords and Access

4.10.1 Staff and line managers are reminded that passwords should never be shared or passed on to other people. This is a breach of the Terms and Conditions of Use as defined in the ICT Acceptable Use Policy and can lead to suspension of the account and possible disciplinary action. Staff must never divulge their passwords and line managers must not ask for them.

4.10.2 If the member of staff leaving has access to other systems or shared resources, the passwords on these should be changed following their departure. This may be particularly pertinent to IT technical staff in schools or departments.

4.10.3 Any other access, such as codes to buildings or doors should also be changed and door access permissions revoked if appropriate.

4.11 Physical Workspace

4.11.1 The physical workspace should be tidied and cleared by the day of departure.

5.0 Internal moves and temporary medium/long term absences

Although the above guidance relates to instances of staff leaving the University, many of the principles will apply to staff who leave one department to join another within the University, or to situations of planned medium or long term absence (e.g. pre-planned medical procedure, maternity/paternity/ parental leave, sabbaticals etc).

Specifically the following sections above should be considered for internal moves between departments:

Section 2	Planning
Section 3	Documents
Section 4.5	Data
Section 4.6	Email
Section 4.7	Specialist applications
Section 4.9	Property
Section 4.10	Passwords and Access
Section 4.11	Physical workspace

The following sections should be considered for temporary absence situations:

Section 2	Planning
Section 3	Documents
Section 4.6	Email
Section 4.7	Specialist applications