IT arrangements for Leavers and their Line Managers

Version Number 1.0

Effective from 01 October 2016

Author: Senior Information Security Officer

Legal, Planning & Governance

1.0 Purpose

This document outlines the information governance and IT access considerations in respect of departing employees (including researchers) or departing workers (including consultants or agency workers) who have a University IT account – collectively referred to in this document as "Leaver". It sets out what should happen before and after the Leaver leaves the University. This document includes the procedure that should be followed where it is known in advance of leaving that the Leaver will require IT account access after their employment/appointment ends. See flowchart at Appendix 1.

2.0 Recommended handover arrangements

Employees and workers must ensure that all relevant information and records are stored and managed appropriately within their team. This is critical to good information management as per the University "*Information Framework"* (see Related Documentation). All Leavers (or workers moving to another role) should discuss with their Line Manager the arrangements they have made for information handover.

Lime Managers and Leavers should ensure that any information and/or documents held in the Leaver's email systems are transferred to other record keeping systems prior to leaving. This helps to retain organisational knowledge and history of decision making.

Information handover arrangements could include some or all of the following:

- Ensuring storage of information in the relevant (and specified) areas of University managed storage facilities. This includes shared network drives, functional email systems or SharePoint.
- Setting up an out-of-office message on the Leaver's email account giving an alternative point of contact e.g. stating "X has now left the University, please send your enquiries to person Y (email address) or person Z (email address) so that your request can be dealt with".
- Removing Leavers from limited access functional email accounts/shared folders/SharePoint.
- Changing passwords on folders containing confidential and sensitive information.

University email accounts **should not** be set to redirect to a personal email account. Any such re-directs will be deleted to prevent unauthorised access to University information.

Mailbox contents should not be copied and kept as personal property: Email is provided for University work purposes and all communications are the property of the University as specified in the ICT Acceptable Use Policy (see Related Documentation section). This principle applies to all employees/workers.

However, private and personal information that might be held in a Leaver's F:\ drive may be taken by the Leaver when they leave. This should be in agreement with an employee's line manager.

In advance of their last day, Line Managers should ensure that the Leaver has complied with the above guidance.

For guidance about access or rights to research material when leaving the University, the Line Manager and / or Leaver should contact the Information Governance team in conjunction with the Research Supervisor and/or Associate Dean Research within the School and the Intellectual Property Manager.

3.0 Default situation on retention of data held in a Leaver's IT account and on their equipment

A Leaver's IT account (which includes V:\ drive, Blackboard, F:\ drive and mailbox) is disabled either on the date the HR SAP entry records the Leaver as ceasing to be employed or, in the case of an associate IT account, on the date given to IT Services by the Leaver's line manager confirming when they will cease to be engaged by the University.

The F:\ drive and mailbox contents are deleted 3 months later. This is documented in the "*Retention of IT System Logfiles"* statement (Related Documentation section).

IT Services manage the erasure and re-image of all University computers and mobile devices before re-issue to another user. As this is usually carried out shortly after the equipment is returned to IT Services, information that may have been saved to the Leaver's C:\ drive cannot be accessed or retrieved after they have left the University.

4.0 Extending Access to an account

There are separate processes for:

a) requesting that a Leaver retains access to their IT account after leaving; and
b) requesting access to a Leaver's IT account after they have left,

These are set out below and are also illustrated in a flowchart at Appendix 1.

4.1 Requesting an extension to a Leaver's account before they leave

In advance of leaving, Leavers should make University work and information available to colleagues and/or their line manager as part of a formal handover. See section 2.0 *Recommended handover arrangements* above.

Be aware that it is not acceptable or appropriate for Leavers to take information that belongs to the University with them when they leave. There may be instances when continuing use of University email or other systems by a Leaver after leaving is justified e.g. an academic member of staff is leaving but will continue to supervise his / her PhD students until the PhD is completed or a replacement supervisor is appointed. Extending access to a Leaver's IT account beyond the end of their employment/appointment has implications for confidentiality and intellectual property. There may also be legal and contractual considerations.

If it is deemed appropriate for an account extension to be put in place, the advance request shall be made as follows:

A. Any Leaver or their line manager who is requesting extension of access to IT resources should make the request formally in writing or email to their Dean of School / Director of Professional Services;

B. This request should set out the business reasons and should specify exactly what access will be required and for how long;

C. The Dean of School / Director of Professional Services should discuss and reach agreement on the request with the relevant HR Business Partner. The HR Business Partner can advise on the HR implications if the extension is requested to enable the leaver to continue carrying out duties connected to their employment / appointment;

D. If the Dean of School / Director of Professional Services decides to refuse the request, he/she should inform the Leaver in writing;

E. If, however, the request is approved, the Dean of School / Director of Professional Services should email the IT Service Desk confirming and authorising the account extension request and the time period;

F. The maximum period for account extensions is three months. Only in the most extenuating of circumstances will this period be extended;

G. The IT Service Desk will then request ITSERT approval;

H. If ITSERT approval is obtained, the IT Service Desk will progress the account extension (until the agreed end date) and notify the Leaver that the access request has been approved and enabled as well as stating the end date of the extended access.

4.2 Requesting an extension to a Leaver's account after they leave

A. Occasionally a Leaver may request access to their mailbox or F:\ drive after they have left the University.

B. If advance approval has not been sought, or has been sought and not granted (see 4.1 above) the Leaver should direct such requests to HR central services following the "*Access requests by Ex-employees to IT accounts*" procedure (Related Documentation section).

C. A line manager or colleague may request operational access to a Leaver's emails or F:\ drive after s/he has left University employment. Any such requests must follow the "*Third party access to IT Accounts Procedure*" (Related Documentation section).

5.0 Related Documentation

The following documents can be found on the University Policy & Procedure pages http://policies.salford.ac.uk/ or under 'P' via the Staff Channel A-Z index.

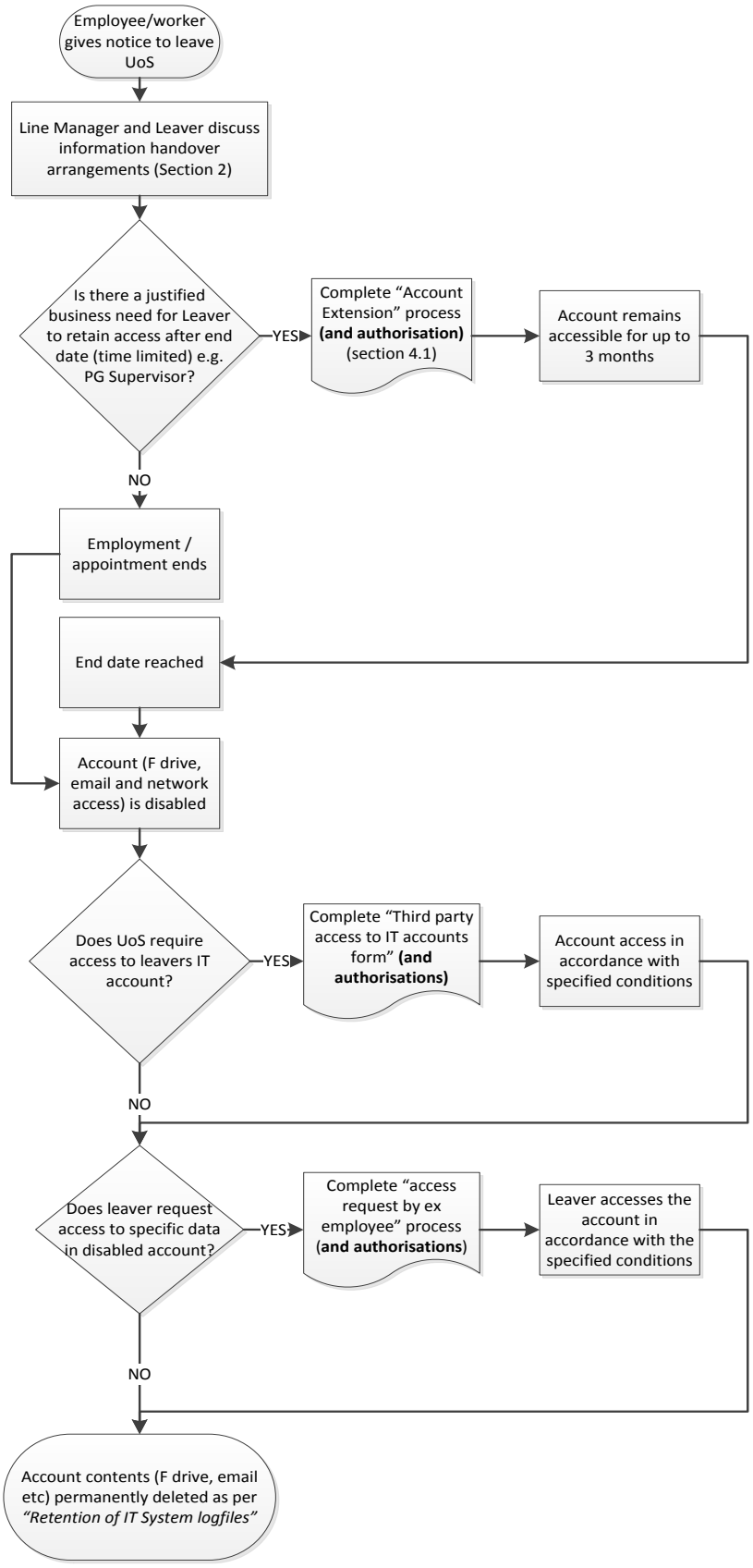
- Information Framework (Information Governance section)
- Intellectual Property Policy (Research section)
- ICT Acceptable Use Policy (Information Technology section)
  - *Retention of IT System Logfiles (Information Technology section)*
  - *Access requests by Ex-employees to IT accounts (Information Technology section)*

The following form can be found on the IT Services webpages http://www.its.salford.ac.uk/servicedesk/

- *Third party access to IT Accounts Procedure (Service desk top forms)*

6.0 Appendices

Appendix 1: Leavers IT arrangements Flowchart



Document Control Information	
Owner: Associate Director IT Services & Head of Information Governance (Legal & Governance) **Author(s):** Senior Information Security Officer	**Reason for Development** New as no previous procedure

Revision History (published versions)

Author	**Summary of Changes**	**Version**	**Authorisation (Role/Board: Date)**
C Price	New document, provides overview of IT access and information security measures before and after staff leave.	V1.0	Head Information Governance: 26/08/2016 & Associate Director IT Services: 19/09/2016

Have you completed formal assessment with the following advisory teams:

Equality Analysis (E&D, HR) Equality Assessment form	1. *June 2016.*
Legal implications (LPG)	2. *23 June 2016 Employment law advice (A. Haddock)* 3. *Version 0.6 seen and agreed by K Watkinson & Gill Hobson (HR)*
Information Governance (LPG)	4. *June 2016 and throughout document development. ITSERT members have also reviewed and amended document.*
Student / Research facing aspects (QEO) (R&E)	5. *N/A* 6. *Version 0.6 seen and agreed by J Cresswell & A Kurien (R&E)*
UKVI Compliance (Student Admin)	7. *N/A*
Review Due	3 years by August 2019
Document Location	University Policy & Procedure pages http://www.salford.ac.uk/policies