UNIVERSITY OF **LIVERPOOL** | COMPUTING SERVICES

Records Management Guidance:
Staff Leaving - Records Checklist

Who should follow this checklist?

If you are leaving the University, or moving to another role within the University, then you must ensure that all records used in your current work are put in order before you leave. Print out and read through this checklist as soon as you know you will be leaving, and set aside to go through it with your line manager and complete the actions required. Your line manager should go through the checklist with you to clarify what needs to be done by you and what they need to do. On the last day, you and your line manager should both sign to confirm that everything is in order.

Why is it important?

It is of vital importance to follow these guidelines to ensure
- Business continuity in the department itself, and across the University
- Accountability of the University for the work of its staff
- Compliance with audit, legal and regulatory requirements (e.g. Data Protection, Freedom of Information)
- Compliance with University records management policies and procedures
- Reduced information and asset security risks

Points to remember

All records (i.e. pieces of information in any format) created or maintained by staff at the University in the course of their work are the property of the University. These include paper documents, electronic documents and data, audio-visual material and emails.

Further Information

- Records Management website: guidance notes, policies
- University Retention Schedule and Records Retention Guide: how long to keep your records
- Computing Services Department Guidance on Staff & Students leaving
- Human Resources Website

Actions to be taken during your last month in post	Date Completed
1. Identify records	
Identify the location of all records created and maintained by you as part of your work. Make a list (if one does not already exist), for your reference and to hand over to your line manager/successor. Remember to check: ➢ Personal storage space on your PC, the M Drive, in your desk, PDAs e.g. University mobile phone, etc. ➢ Email accounts (includes personal and shared email) ➢ Shared electronic and paper filing systems of the section ➢ Records in storage e.g. in University Records Centre or other locations ➢ Home storage. *N.B. It is not normal practice to store University records at home.*[1]	
2. Destroy records that are no longer needed	
Identify all records which do not need to be kept, and arrange for their destruction. This action should be recorded in an audit trail if appropriate. ➢ Non-confidential papers should be placed in the recycling bins. ➢ Confidential papers should be placed in secure waste consoles if available, or disposed of via Records Management. ➢ Non-paper waste such as CDs, old USB pens, or photographs should be disposed of via Records Management. ➢ Electronic waste material such as old files, documents and emails should be deleted. In particular, make sure to delete your own personal data e.g. copies of your CV. ➢ Redundant IT equipment should be collected by the IT Asset Disposal Service.	
3. File records which need to be kept	
File all records ensuring they have clear and accurate titles (see file naming guidance): ➢ Agree steps with your line manager to maintain access and security arrangements, and ensure that confidential and sensitive material is protected. For example, confidential information and emails could be forwarded to the most appropriate colleague, or saved in a location where appropriate access restrictions are in place. ➢ Add all other files to the shared paper and electronic filing systems, or send to semi-current storage if appropriate. If shared filing systems do not exist, then ask your line manager for instructions. Records must not simply be dumped into drawers, or onto CDs and other devices. ➢ Save emails which contain corporate information onto the correct place on the shared drive, or into your section's email account, with meaningful titles. ➢ Where possible note the recommended retention period with the files.	
4. Inform line manager about any additional roles	
Inform your line manager if you hold any additional roles on behalf of the department e.g. if you are a Freedom of Information contact or sustainability officer, so that another member of staff can be appointed to this role.	

---

[1] Any University records stored at home must be returned or transferred back to the University. Hard copy records must be returned to your section. Electronic records must be put onto the University Network/environment/MWS. You should delete or destroy personal copies of such information unless you have been given permission to retain them. N.B. If you have high risk sensitive information or personal data stored on a personal computer it may be necessary to destroy the hard drive. See CSD Policies.

Actions to be taken during your last week in post	Date Completed
1. Hand over records to other staff in the section	
➤ Hand over all records to the appropriate member(s) of staff, as agreed with your line manager, with lists detailing locations of any records held elsewhere (e.g. records held in the Records Centre). ➤ Try to give as much additional information about the records, e.g. their main purpose, the retention recommendations, any security concerns.	
2. Arrange for return of University records and equipment	
➤ Return any records checked out from electronic systems (e.g. VOCAL), filing cupboards, the Records Centre etc. ➤ Return any other University equipment e.g. mobile phone, laptop.	
3. Take action to maintain security and access arrangements	
➤ Return all filing cabinet and safe keys, and give all passwords and/or encryption codes used to protect documents to your line manager. ➤ Ask your line manager to make arrangements to disable any privileged computing rights. Also if your University account will be needed for longer than the usual 2 month extension period, your line manager should inform the Computing Services Department Helpdesk. ➤ Do not remove any records, except your personal papers and effects. If there are records that you want to take copies of, get permission from your line manager, as records created by you as part of your job belong to the University. Original records should never be removed from the University. There are some records which it is not appropriate for former employees to have access to.	

Actions to be taken on your Last day	Date Completed
1. Do final checks on your email account and telephone	
➤ Pass details of any emails or phone messages which you have not had time to deal with to your line manager for reassignment. ➤ Set an out of office message on your email account with contact details of a colleague/ your section, so that enquiries are redirected. ➤ Delete your personal voicemail, greeting, and any other messages from your phone.	
2. Check that all personal information has been removed	
Remember to check all of the following locations: ➤ Your desk drawers/other physical storage space. ➤ The M Drive, your computer hard drive, emails and internet explorer 'favourites'.	
3. Take final actions to maintain security and access arrangements	
➤ Return and cancel staff card and keys. ➤ Ask your line manager to ensure that proximity/alarm, password, and key holder access to all relevant locations is disabled.	

Signature to confirm that all actions have been completed	Date
(Employee)	
(Line Manager)	