DEPARTMENT OF STATISTICS

UNIVERSITY OF OXFORD

TITLE	**Account Closure Policy**		
DATE Year	2025		
AUTHOR(S)	Name, Role	Date	Signature
	Stuart, McRobert		
LAST REVIEWED DATE		10 Feb 2025	
NEXT REVIEW DATE		2027	
RELATED POLICIES			
DOCUMENT HISTORY	Valid from	Changes	
	Today	Upgrade	

Overview

When a user leaves the department their computing account must be closed and any files optionally transferred prior to deletion. Any departmentally supplied computing equipment and department-licensed software needs to be returned either for reallocation or disposal.

Please note changes to a user's University card status (including expiry) can trigger **immediate** (e.g. next day) termination of campus SSO and hence access to Nexus email, eduroam Wi-Fi, VPN, and anything else authenticated by SSO. Details about finishing at Oxford can currently be found on this IT Services web page.

This isn't something department IT staff can prevent, instead users need to contact e.g. their College or Department **administration** to update their **University card** expiry date and/or status if remaining associated with Oxford. If a user's SSO is about to expire, short SSO extensions can be requested through the SSO Account Access Extension service request page.

Purpose

The purpose of this policy is to effectively manage computing resources, maintain account security, and to avoid the inadvertent loss of user files and research data.

Scope

The scope of this policy is to define the policy by which authorised user accounts are closed and associated files and computing equipment are managed when a user leaves the department. This policy pertains to all computer systems, hardware, software and firmware owned and/or operated by the department.

Policy

Authorised users planning to leave the department need to arrange several things prior to their departure, including:

- The transfer of any of their files which they may require and are entitled to securely transfer to another site and/or to removable media e.g. secure USB drive(s).
- The transfer of any files to colleagues and/or their supervisors.
- The proper deletion of any remaining confidential material.
- The deletion of files no longer required on computational servers.
- Arrange for the return of any computing equipment supplied by the department.

As a precaution, IT will when notified of their departure, collect and store the authorised user's departmental computer (if they have one) for no more than one month, prior to disposal or reallocation.

The authorised user's account will then be set for closure and file deletion in a timely manner, unless approved by the Head of Department to remain open, e.g. for collaboration.

Timeline

The following timeline is specified:

- One month prior to departure:

- o Users should arrange with colleagues and/or their supervisor for the transfer of files, including those stored on departmental and research servers, desktops and any other storage devices to avoid any loss of important data e.g. as required for research papers and publications.
- o Remember to also arrange for any data stored on other systems associated with your Oxford SSO, e.g. ARC, OneDrive etc to be transferred/reassigned/removed prior to SSO access expiring.
- o This will help avoid supervisors or colleagues being unable to access important work.
- o The Academic Administrator will promptly notify IT regarding the user's departure date and the arrangements in place.
- o Users should plan the safe secure transfer of any of their files which they may require and are entitled to transfer to another site and/or by using removable media e.g. secure USB drive(s). With large volumes of data this can take a considerable amount of time to complete. Making duplicate copies is also a good idea.
- o Users should also plan the safe deletion of any confidential material no longer required.
- A week prior to departure users should:
  - o Make sure IT know your non-Oxford email address should they need to contact you after leaving.
  - o Confirm arrangements for the return of **all** computing equipment supplied by the department.
  - o Be aware that after departure the computer desktop they may have been using will be removed and any data stored there will no longer available, even from backups after just a few months. Once their Statistics account has been closed, any files owned by that account will be deleted. Users should not expect IT to be able to recover files after they have left.
  - o SSO termination can quickly trigger closure and deletion of files on other systems, e.g. Nexus email.
  - o Check all confidential material has indeed been deleted or ownership transferred to another appropriate authorised user.
- After departure, IT will:
  - o Collect any IT equipment for storage of no more than one month, prior to disposal or reallocation.
  - o Close the user's account in a timely manner with email reminders sent clearly indicating the planned account closure date, unless approved to remain open, e.g. by Head of Department for collaboration (with status changed to visitor).
  - o Once an account has been closed, files and backups owned by that user will automatically expire over the coming months, and users should not expect IT to be able to restore them again.
  - o Department webmaster will normally remove entries for that user following their departure.

Enforcement

Where this policy is found not to have been followed, corrective action should be taken to promptly achieve compliance and the computing manager notified. The computing manager may notify the chair of the computing committee, especially where further disciplinary and/or other action may be considered appropriate.

Definitions

- **Authorised user** – A user authorised by the department to be using the computing facilities provided.
- **Computing equipment** – includes computers (desktops, servers, laptops, tablets and similar devices), PDAs, smartphones, network devices, computer peripherals.

Revision History

- November 2011 – Discussion at computing committee (CC) meeting
- February 2012 – Draft discussed at CC, to be extended to encompass other aspects of account closure, particularly timings.
- May 2012 – Revised policy draft with timeline. Approved at CC.
- February 2025 – Policy updated to reflect changes over the past decade, draft to CC.