



# M365 Account Deletion Policy

## 1. Purpose

- 1.1 This document sets out The London School of Economics and Political Science ("the School")'s policy on deletion of Office365 accounts along with their associated documentation.
- 1.2 If you have any questions relating to this policy please contact the School's Information and Records Manager, Rachael Maguire, [r.e.maguire@lse.ac.uk](mailto:r.e.maguire@lse.ac.uk).

## 2. Background to this Policy

- 2.1 The School has a need to manage M365 accounts, so that those belonging to staff and students no longer at the School are not kept forever. M365 accounts cover Outlook, SharePoint and Teams sites, OneDrive and Teams Chat, all of which contribute to the School's storage quota. As such, the School needs to ensure that in order to not pay for large amounts of extra storage that accounts and any files within these accounts no longer needed are regularly deleted.
- 2.2 Information held in M365 accounts that are no longer in use are still subject to Freedom of Information and Data Protection legislation. This is another reason the School needs to ensure that it is not still holding information it no longer needs.
- 2.3 Definitions of terms used in this policy:
  - 2.3.1 'M365 account' means the individual staff or student space provided by the School for the purposes of use and storage of electronic mail or documents.
  - 2.3.2 'Associated documentation' is the emails, SharePoint sites, documents, spreadsheets, presentations, etc stored within the M365 accounts.

## 3. Policy

- 3.1 The School will delete M365 accounts and all associated documentation at the end of a user's connection with the School.
- 3.2 Current schedules for account suspension and deletion are outlined in Appendix A: DTS network account creation and deletion dates.

## 4. Responsibilities

- 4.1. DTS will delete the M365 accounts and all associated documentation in line with the policy statement in Section 3.1.
- 4.2. All staff and students leaving the School must transfer any associated documentation out of their specific M365 account storage (Outlook and OneDrive) before the deadline given in Section 3.1.
- 4.3. Human Resources are responsible for informing DTS of staff leaving dates in a timely fashion.
- 4.4. The departmental managers of academic departments, centre managers of research centres or heads administrative divisions are responsible for ensuring that DTS are informed of the leaving dates of any short term non-permanent staff members.

## 5. Compliance, Policy Awareness and Disciplinary Procedures

- 5.1 Any breach of this policy will be handled in accordance with all relevant School policies, including the *Conditions of Use of IT Facilities at the LSE* and the appropriate disciplinary policies.

## 6. Status Of This Policy

This Policy has been approved by Data and Technology Management Board on 23/1/2024. It is available in the policies and procedures section of the website.

## Appendix A: DTS Network Account Creation And Deletion Dates

The following table indicates the times of the year during which accounts for different types of user are typically created, expired and deleted.

Expiry of an account prevents logon and use of the account but keeps the account in the system.

An expired account can be re-enabled and this is common for returning students e.g. summer school students returning as undergraduates or postgraduates, or undergraduates returning as postgraduates.

Through the Lent term expired accounts are check ahead of large deletion batches of student and other accounts at the end of the term, thus purging the system of old accounts ahead of the new student account creations in the summer.

User Type	Creation	Expiry	Deletion
Staff	All year round. At the time a member of staff joins, from information fed by the HR Resource Link system.	1. Manual. 2. At the end of the last month of the contract.	Two months after expiry (in the absence of attached generic accounts).
Student: UG	Sep-Oct From information fed by the SITS student records system	December of the last year of study.	March (Allows for re-sits).
Student: Taught PG	Jul-Dec From information fed by the SITS student records system	December of the last year of study.	March (Allows for re-sits).
Student: Research PG	Jul-Nov	December of the last year of study.	March
Student: Exec MSc	Each term for 1 year	December of the last year of study.	March
Student: Short Course	Start and finish throughout year	Created with duration of between 2 weeks and 20 months.	Two months after expiry
Student: Summer School	May -Jul	August end	March (due to high correlation with degree applicants).
Student: Exec Summer School	May-Jan	End of the last month of study.	Two months after expiry
Generic	All year round	Manual	March

Note that there is no definitive end date for taught students and Exec MSc students and expiries are based on assumptions of when courses are completed.

## Document control

### Version history

Date	Version	Comments
28/4/2017	1.0	Information Security Advisory Board 4/5/2017
7/12/2017	2.0	Office 365 Governance Board 7/12/2017
31/1/2018	2.1	Circulated to Information Governance Board members
11/1/2024	3.0	Data and Technology Management Board 23/1/2024

**Changes from previous version: Service title changes (Office 365 -> M365), Division title changes (IMT -> DTS), clarification of descriptions. No changes to policy.**

### Contacts

Position	Name	Email	Notes
Director of Cyber Security & Risk Management	Jethro Perkins	<a href="mailto:j.a.perkins@lse.ac.uk">j.a.perkins@lse.ac.uk</a>	

### Communications and Training

Will this document be publicised through Internal Communications?	Yes - website
Will training needs arise from this policy	No
If Yes, please give details	