

Recovering Evidence From Deleted Microsoft 365 User Accounts

Microsoft 365 user accounts pass through recoverable states with clocks attached after deletion. Understanding soft deletion, inactive mailboxes, and hard deletion is crucial for evidence recovery. This guide outlines preservation and collection strategies, including reconstruction from the wider estate when an account is gone, and addresses legal consequences of leaver processes.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.

<https://e-discovery.uk/library/recovering-evidence-from-deleted-microsoft-365-user-accounts>

DELETEDM365ACCOUNTS · A GUIDE FOR UK LAWYERS Recovering Evidence from Deleted Microsoft 365 User Accounts Soft Deletion, Inactive Mailboxes, Retention and the Leaver Who Left Before the Hold COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES DELETED-ACCOUNT RECOVERY

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the leaver process is a deletion engine 03 The lifecycle of a deleted account: soft deletion, inactive state, hard deletion 04 What survives where: mailbox, One Drive, Teams, audit logs and licences 05 Preservation and collection before and after the clocks run 06 When the account is gone: reconstruction from the rest of the estate 07 Leaver processes and preservation duties: the legal consequences 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: ADELETEDMICROSOFT365ACCOUNTPASSESTHROUGH RECOVERABLESTATESWITHCLOCKSATTACHED: KNOWTHESTATE, ACTINSIDETHE CLOCK, ANDWHENTHECLOCKHASRUN, RECONSTRUCTFROMTHEESTATETHEUSER COULD NOT TAKE WITH THEM

§ 02 · FIRST PRINCIPLES The problem in plain English: the leaver process is a deletion engine

§ 03 · THELIFECYCLE The lifecycle of a deleted account: soft deletion, inactive state, hard deletion

§ 04 · WHATSURVIVESWHERE What survives where: mailbox, One Drive, Teams, audit logs and licences

§ 05 · BEATINGTHECLOCKS Preservation and collection before and after the clocks run

§ 06 · AFTERTHECLOCKS When the account is gone: reconstruction from the rest of the estate

§ 07 · THELEGALFRAME Leaver processes and preservation duties: the legal consequences

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE
MAILBOX RETENTION DIRECTORY SOFT- DELETED / COUNTERPARTS + BACKUPS
RESTORED SHARED STORES + DEVICES USER INACTIVE ONEDRIVE AUDIT / (HOLD)
STAGE LAYER

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THERESTOREONDAYTWENTY - SIX
EXAMPLE2 · THECUSTODIANREBUILTFROMEVERYONEELSE EXAMPLE3 ·
THELEAVERPROCESSTHATRANAFTERTHELETTER

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes
Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask
your client Ask your opponent Ask your e Discovery / forensic provider ANDPOLICIES

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The
deleted-account checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions IT deleted the account last week. Is
the data gone? What is an inactive mailbox and how do we get one? The account was
hard-deleted a year ago with no hold. What now? Our leaver process deleted a relevant account
after the dispute began. How bad is it? Doesn't UK GDPR require us to delete leavers' data? Can
we tell whether the opponent's deleted custodian is really unrecoverable?

§ 14 · REFERENCE Glossary Sources and authoritative references 31 · CPR Part 35:
justice.gov.uk, Part DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab
Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB
NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

IT deleted the account last week. Is the data gone?

Almost certainly not yet: the account is soft-deleted and restorable in full for the platform's window (currently 30 days), One Drive has its own retention period, and any hold in place has made the mailbox inactive (§3). Restore today, hold, collect: Example 1's sequence. The answer changes with every day of delay.

What is an inactive mailbox and how do we get one?

A mailbox preserved after its user is deleted because a litigation hold or retention policy applied at deletion: no user, no licence, contents searchable and exportable for the hold's life. It is created by holding the mailbox before deletion, or by restore-hold-delete inside the soft-deletion window (§5): the mechanism a litigation-aware leaver process invokes for anyone relevant.

The account was hard-deleted a year ago with no hold. What now?

Reconstruction (§6): the custodian's correspondence from counterparts' mailboxes and external parties, their work product from shared stores, their chats from other members' copies, their activity from audit logs, and their stores from backups and devices where they exist: Example 2 rebuilt a central custodian this way with measured coverage. The account's stores are gone; the footprint largely is not.

Our leaver process deleted a relevant account after the dispute began. How bad is it?

It depends on the duty date and what remains: deletion after contemplation is a preservation failure (§7) whose consequences scale with the gap and its explanation: mitigated substantially by prompt, honest reconstruction and candid evidence about the process. Fix the process now for every other custodian; the second deletion is the one that turns a failure into a pattern.

Doesn't UK GDPR require us to delete leavers' data?

It requires minimisation in the ordinary course and permits retention where legal claims require it: both branches, documented: a leaver process needs a litigation-pause step precisely so that the ordinary branch does not run when the exceptional one applies (§7). Citing GDPR for a deletion after contemplation concedes the duty was known and not met.

Can we tell whether the opponent's deleted custodian is really unrecoverable?

Ask §11's questions: account state, hold status at deletion, One Drive and audit retention, and reconstruction attempted: the answers either evidence a genuine hard deletion with honest reconstruction, or reveal windows that were open and unused, holds that never reached the leaver, and a §6 effort never made: Example 3's application was built on exactly that gap between what the platform allowed and what the opponent did. cflab. u k · e-discove r y. u k

©2026 Computer Forensics Lab Ltd · cflab.uk · e-discovery.uk · info@cflab.uk · +44 (0)20 7164 6915 Page 15 of 17

Source: <https://e-discovery.uk/library/recovering-evidence-from-deleted-microsoft-365-user-accounts>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.