COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Recovering Evidence from Deleted Microsoft 365 User Accounts

Soft Deletion, Inactive Mailboxes, Retention and the Leaver Who Left Before the Hold

The custodian who matters most is very often the one who has already left: the departed director, the dismissed employee, the contractor whose engagement ended: and their account was deleted by a leaver process that ran exactly as designed. What survives depends on a set of Microsoft 365 mechanisms most organisations have never mapped: the soft-deletion window, the inactive-mailbox state that holds create, the retention policies that keep content after the account is gone, OneDrive's post-deletion retention, and the audit trails that outlive the user. Some of these windows are days; some are years; all are configurable and none pause for a dispute. This guide explains for UK lawyers how deleted-account data survives, in what states and for how long, how to preserve and collect it before the clocks run out, what to do when they already have, and how to challenge an opponent whose leaver process deleted a key custodian a week before the letter of claim.

⏱ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its eDiscovery arm, **e-discovery.uk**, is instructed on deleted-custodian problems weekly: the hold that arrived after the leaver process, the inactive mailbox nobody knew existed, the OneDrive on its last day of retention: and the laboratory side reconstructs what the tenant lost from the sources that remain. The mechanisms in this guide are the ones those instructions turn on.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | DELETED-ACCOUNT RECOVERY | RETENTION & HOLD MAPPING | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: A DELETED MICROSOFT 365 ACCOUNT PASSES THROUGH RECOVERABLE STATES WITH CLOCKS ATTACHED: KNOW THE STATE, ACT INSIDE THE CLOCK, AND WHEN THE CLOCK HAS RUN, RECONSTRUCT FROM THE ESTATE THE USER COULD NOT TAKE WITH THEM

The lifecycle (§3): deleting a user places the account in a soft-deleted state (currently 30 days) from which it can be restored intact; a mailbox under a hold or retention policy at deletion becomes an *inactive mailbox*, preserved for as long as the hold lasts and searchable by compliance tooling even though no user exists; a mailbox without a hold is deleted with the account after the soft-deletion window; OneDrive content is retained for a configurable period after deletion (a default of 30 days, commonly extended by policy) with a further recycle stage; Teams private-channel compliance copies live in the mailbox and follow its fate (guide 101); and audit logs, sign-in records and directory history persist under their own retention regardless of the account. **Preservation (§5):** the fastest actions are the ones that convert the clock into a hold: restoring a soft-deleted user, placing a hold that turns the mailbox inactive, extending OneDrive retention, and exporting audit logs: with the leaver process itself paused for relevant custodians the moment a matter is contemplated, per guide 97 §3. **Reconstruction (§6):** where the clocks have run, the account's contents survive in counterparts (recipients' mailboxes, shared sites, other members' Teams copies), in backups and archives, in the audit layer, and on devices: guide 95's method applied to a whole custodian. **Legal consequences (§7):** a leaver process that deleted a relevant custodian after the preservation duty arose is a preservation failure with guide 95 §6-§7's consequences; one that ran before is a gap to be explained with the policy evidence: the date of contemplation, again, decides which.

- **Soft deletion is reversible:** a restored user comes back whole: the 30-day window is the cheapest recovery in the platform.
- **Holds create inactive mailboxes:** a hold at deletion preserves the mailbox indefinitely: the mechanism the leaver process must invoke.
- **OneDrive has its own clock:** separate retention, separate recycle, separate export: mapped separately.
- **Audit logs outlive users:** what the account did survives what it held: the reconstruction spine.
- **The duty dates the failure:** deletion after contemplation is spoliation; before, a gap with an explanation: the policy file decides.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the leaver process is a deletion engine

Every organisation has a leaver process, and every well-run one deletes accounts on schedule: licences cost money, dormant accounts are security risks, and data-protection law rewards minimisation. The process is correct. It is also, from a disclosure standpoint, an automated destruction routine pointed at exactly the custodians litigation most often needs: the people who left because of the dispute, or whose departure caused it. The account deleted "30 days after termination" was deleted 30 days after the event the claim is about.

Microsoft 365 mitigates this in ways that are powerful and poorly understood: the deletion is staged, holds convert deletion into preservation, and much of what the user did survives in logs and other people's data. But the mitigations are windows and configurations, not guarantees: and the organisation that discovers the mechanism after the window closed has a gap to explain. This guide is the map of the windows, the actions that convert them into holds, and the reconstruction that remains when they are gone: the guide 95 method with a Microsoft 365 manual attached.

§ 0 3 · THE LIFECYCLE

The lifecycle of a deleted account: soft deletion, inactive state, hard deletion

- **Active with licence removed:** a common first step: the licence removed but the account retained: mailbox and OneDrive may enter retention-driven deletion timelines even before the account is deleted: the pre-deletion clock many leaver processes start without realising.
- **Soft-deleted (currently 30 days):** the deleted user sits in the directory's recycle bin; restoring the user restores mailbox, OneDrive, group memberships and Teams data as they were: the whole custodian back, intact, with one administrative action inside the window.
- **Inactive mailbox:** if a litigation hold or retention policy applied to the mailbox at deletion, the mailbox is retained as inactive: no user, no licence, contents preserved for the hold's duration, searchable and exportable through Purview eDiscovery: the state that makes departed custodians collectable years later, and the state a leaver process should create for anyone relevant.
- **Hard-deleted:** past the soft-deletion window without a hold, the mailbox is permanently removed (subject to any remaining retention-policy hold on content); OneDrive follows its own retention period and recycle stages before permanent deletion: after which the account's own stores are gone and §6 begins.
- **The clocks in summary:** soft deletion (days), OneDrive retention (configurable, commonly 30 days to years), recycle stages (days to months), audit-log retention (months to years by licence): each verified for the tenant, because defaults are changed and platform behaviour moves.

§ 0 4 · WHAT SURVIVES WHERE

What survives where: mailbox, OneDrive, Teams, audit logs and licences

- **Mailbox:** the primary store: mail, calendar, contacts, Teams chat compliance copies (one-to-one and group chats, private-channel messages per guide 101): preserved as inactive under hold, or lost with the account: including the recoverable-items folders whose deleted-item retention guide 95 relies on.
- **OneDrive:** personal files with version histories (guide 102) and sharing records: retained post-deletion for the configured period, with a secondary admin or manager access route during it; then recycle; then gone: the store most often lost because its clock is separate from the mailbox's.
- **Teams and SharePoint:** standard-channel content lives in team stores and survives the member's deletion; private-channel copies in the deleted user's mailbox follow the mailbox's fate; files the user contributed to shared sites survive in those sites regardless: the distributed design of guide 101 working in reconstruction's favour.
- **Audit and sign-in logs:** unified audit log entries (actions, files, shares, deletions), Entra sign-in and directory audit records: retained by licence tier and policy independently of the account: the record of what the user did, surviving the deletion of what they had.
- **Directory and licence history:** account creation, role assignments, group memberships and licence changes recorded in directory audit data: the custodian's existence and lifecycle proven even when content is gone: guide 95's existence evidence for an entire account.

§ 0 5 · BEATING THE CLOCKS

Preservation and collection before and after the clocks run

- **Pause the leaver process:** on contemplation of a matter, relevant leavers' accounts are exempted from deletion (guide 97 §3): the single most valuable control, and one most organisations have to add to their process after the first loss.
- **Restore soft-deleted users:** inside the window, restoration brings the whole custodian back: then hold, then collect, then (if the business insists) delete again under a hold that creates an inactive mailbox: the sequence that converts a near-miss into a preserved source.
- **Create inactive mailboxes deliberately:** holds applied before deletion; where the account is already soft-deleted, restore-hold-delete achieves the same: verified by confirming the mailbox appears as inactive and is searchable.
- **Extend OneDrive retention and export early:** the post-deletion retention period extended by policy where possible; otherwise the OneDrive content exported through the secondary access route or compliance tooling before its clock runs: with version histories included per guide 102 §5.
- **Export audit and directory logs now:** the account's action history, sign-ins and directory events pulled before their own retention expires: the reconstruction spine collected while it exists, whatever the content stores' fate.

§ 0 6 · AFTER THE CLOCKS

When the account is gone: reconstruction from the rest of the estate

- **Counterpart mailboxes:** every email the user sent or received has another end; internal counterparts' mailboxes (held) reconstruct the correspondence; external counterparts through the parties or third-party routes: guide 82-83's duplicate and thread structures as the recovery method for an entire custodian.
- **Shared stores:** team sites, shared mailboxes (guide 104), group and channel content, DMS: the user's contributions to shared repositories survive their account: often the bulk of their substantive work product.
- **Other members' Teams copies:** group chats and private channels reconstructed from remaining members' mailboxes (guide 101 §6): the user's own messages present in others' compliance copies for every conversation they shared.
- **Backups, archives and journaling:** tenant backups, third-party backup services and email journaling (where deployed) hold the account as it was at backup or transit time: scoped and restored for the specific custodian, proportionality argued on the §4 existence evidence.
- **Devices and caches:** the leaver's laptop and phone (if retained) hold offline mailbox caches, OneDrive sync copies and Teams client databases: guide 97 §3's sequestration paying its dividend: the account's contents on hardware the deletion never touched.

§ 0 7 · THE LEGAL FRAME

Leaver processes and preservation duties: the legal consequences

- **The duty and the date:** PD 57AD's preservation duty arises on contemplation and expressly reaches former employees' documents; deletion after that date under a leaver process is a preservation failure whatever the policy said: guide 95 §6's framework, with the policy's execution logs proving which side of the date the deletion fell.
- **Before contemplation:** deletion under a documented, consistently applied policy before any duty arose is retention, explained from the policy file and the leaver records: guide 95 Example 3's defence, for accounts.
- **Hold-notice reach:** holds and notices addressed to former employees' data as well as current: the mechanism by which the duty is discharged, and the record that shows it was.
- **Data-protection tension resolved:** UK GDPR minimisation supports deletion in the ordinary course and permits retention where litigation requires it: the leaver process needs both branches, documented: the "we deleted it because GDPR" defence fails where a duty had arisen.
- **Consequences and remedies:** specific disclosure of reconstruction efforts, evidence about the deletion's circumstances, adverse inference where the timing and selectivity support it, costs: guide 95 §7's ladder, with the audit and directory logs as the timeline evidence: and, for the party facing its own gap, the honest §6 reconstruction as the mitigation.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a deleted account's evidence is spread across states and stores with different clocks, and the map is worked in clock order. Inside the platform: the soft-deleted user (days), the inactive mailbox (the hold's life), OneDrive's post-deletion retention (configurable), recycle stages, and the audit and directory layer (licence-dependent, independent of the account). Beyond the account: counterpart mailboxes and external correspondents, shared and team stores, other members' Teams copies, tenant and third-party backups, journaling, and the leaver's devices. When the primary path is closed: hard-deleted without a hold, OneDrive past retention, backups rotated: the table names what remains and what it can prove. The account is one custodian; the estate is redundant around every custodian by design, and the reconstruction of §6 is that redundancy read systematically.

EVIDENCE	SOFT-DELETED / RESTORED USER	INACTIVE MAILBOX (HOLD)	ONEDRIVE RETENTION STAGE	AUDIT / DIRECTORY LAYER	COUNTERPARTS + SHARED STORES	BACKUPS + DEVICES
Email + calendar	Y: whole, inside window	Y: for the hold's life	n/a	Actions, not content	Y: the other end	Y: as at backup / cache
Personal files + versions	Y	n/a	Y: inside retention	File operations	Shared copies	Sync copies, backups
Teams chats + private channels	Y	Y: compliance copies	n/a	Channel events	Y: other members' copies	Client databases
What the user did	n/a	n/a	n/a	Y: the surviving spine	Recipients' records	Endpoint artefacts
That the account existed, when	Recycle-bin entry	Mailbox properties	n/a	Y: creation to deletion	Address in headers	Profile artefacts

Fallback strategy in one line: restore inside the window, hold to create the inactive mailbox, export OneDrive and logs before their clocks: and when all have run, rebuild the custodian from counterparts, shared stores, other members' copies, backups and devices.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE RESTORE ON DAY TWENTY-SIX

A director resigned amid allegations that became a claim eleven days later. IT had deleted his account on the standard schedule the day after departure. The instruction came on day twenty-six of the soft-deletion window: the examiner's first action was the restore, returning mailbox, OneDrive, Teams data and group memberships intact; the second was a litigation hold on the restored mailbox and an extension of OneDrive retention; the third was full collection with version histories and audit export. The account was then deleted again, this time into an inactive mailbox that outlived the proceedings. Four days later the window would have closed and §6's reconstruction would have replaced a complete custodian with a partial one. The example is the guide's entire first section: know the state, act inside the clock.

EXAMPLE 2 · THE CUSTODIAN REBUILT FROM EVERYONE ELSE

A procurement manager's account had been hard-deleted fourteen months before a fraud claim in which she was the central actor: no hold, no inactive mailbox, OneDrive long past retention. The §6 reconstruction did what the platform could not: her internal correspondence rebuilt from seven colleagues' held mailboxes (the counterpart layer covering 91% of her sent items by the guide 82 hash census against surviving references); her supplier emails obtained from the suppliers under CPR 31.17; her group-chat contributions recovered from other members' Teams compliance copies; her contributions to the procurement SharePoint site intact with version ladders naming her account; and the unified audit log, retained under the tenant's extended policy, supplying eighteen months of her file and sharing activity. The rebuilt custodian supported the claim's key allegations; the report stated the reconstruction's coverage and its gaps honestly. The deletion had removed her stores, not her footprint.

EXAMPLE 3 · THE LEAVER PROCESS THAT RAN AFTER THE LETTER

An opponent's disclosure omitted a former sales director's mailbox: "deleted under our standard leaver process". The §11 requests drew the records: the letter before claim had been received on 4 March; the director's account had been deleted on 19 March under a process that ran 30 days after termination; the hold notice had been issued on 6 March and had not named former employees' accounts; and the tenant's audit log showed the deletion executed without any hold in place. The duty had arisen before the deletion; the process had not been paused; the hold had not reached the leaver. The specific disclosure application secured a §6 reconstruction at the opponent's cost, an order for evidence about the deletion, and a costs order: with adverse inference reserved to trial on the reconstruction's gaps. The policy was standard; the timing made it spoliation.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The leaver process never paused:** Example 3's timing: deletion on schedule after the duty arose.
- **Holds that miss former employees:** the notice addressed to current staff only; the leaver's mailbox deleted unheld.
- **The soft-deletion window wasted:** the restore available for weeks while correspondence was exchanged: Example 1's counterfactual.
- **OneDrive's separate clock ignored:** the mailbox made inactive, the files lost on their own schedule.
- **Licence removal starting clocks:** retention-driven deletion beginning at licence removal, before anyone thought the account was "deleted".
- **Audit logs left to expire:** the reconstruction spine unexported while the content stores were argued over.
- **"GDPR made us" as the explanation:** minimisation cited for a deletion after contemplation: the defence that concedes the duty was known.
- **Reconstruction not attempted:** the gap pleaded as total when §6 would have rebuilt most of it: guide 95 §10's error, at custodian scale.

Technical limitations

- **Windows are the platform's to change:** soft-deletion periods, retention defaults and tooling scope move: verified for the tenant and date, per this series' standing rule.
- **Hard deletion is hard:** past the windows without a hold, the platform's stores are gone: §6's alternates or nothing, stated honestly.
- **Inactive mailboxes depend on the hold:** a hold that lapses releases the mailbox to deletion: hold management is preservation management.
- **Audit depth is licence-bound:** retention and detail of logs vary by tier (guide 105's caveat): the reconstructable footprint depends on yesterday's subscription.
- **Reconstruction has coverage, not completeness:** the rebuilt custodian is measured against surviving references (Example 2's 91%): the report states the metric and the residual gap.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Which relevant people have left, when were their accounts deleted, and what state is each account in now: soft-deleted, inactive, hard-deleted?
- What are the tenant's soft-deletion, OneDrive retention and audit-log retention settings, and does the leaver process have a litigation-pause step?
- Are the leavers' devices still in IT's possession?

Ask your opponent

- Please identify all custodians relevant to the issues whose accounts have been deleted, stating for each the date of deletion, whether a hold or retention policy applied at deletion, whether an inactive mailbox exists, the OneDrive retention status, and the audit-log retention applicable.
- Please state the date on which your client's preservation duty was engaged, the date and scope of any hold notice (including whether it extended to former employees' data), and whether the leaver process was suspended for relevant custodians.
- Please confirm what reconstruction has been undertaken for deleted custodians from counterpart mailboxes, shared stores, backups and devices, with the results.

Ask your eDiscovery / forensic provider

- Which clocks are still open for each deleted custodian, and what action converts each into a hold today?
- Has the audit and directory layer been exported before its own retention runs?
- What is the reconstruction coverage for hard-deleted custodians, measured how?

SUGGESTED WORDING · LEAVER-PROCESS PRESERVATION CLAUSE FOR HOLD NOTICES AND POLICIES

> "With effect from [date], the standard account-deletion and leaver process is suspended for the individuals listed in Schedule 1 and for any current or former employee whose documents may be relevant to [the matter]. No account, mailbox, OneDrive or Teams data of such individuals shall be deleted, de-licensed or subjected to retention-driven removal without written confirmation from [instructing solicitors]. Where such an individual's account has already been deleted, IT shall immediately: (1) restore the account if within the soft-deletion window; (2) apply a litigation hold to the mailbox so that it is preserved as an inactive mailbox; (3) extend OneDrive retention and export the OneDrive content with version histories; and (4) export the unified audit log, sign-in and directory audit records for the account. Devices issued to such individuals shall be retained unpowered pending forensic imaging."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The deleted-account checklist

- ☐ Relevant leavers listed with deletion dates and current account state
- ☐ Leaver process suspended for relevant custodians, in writing
- ☐ Soft-deleted users restored inside the window
- ☐ Holds applied to create inactive mailboxes; status verified
- ☐ OneDrive retention extended; content exported with versions
- ☐ Audit, sign-in and directory logs exported now
- ☐ Leavers' devices sequestered unpowered
- ☐ Hold notices extended to former employees' data
- ☐ Reconstruction from counterparts, shared stores, backups scoped for hard-deleted custodians
- ☐ Coverage metric and gaps stated in the methodology

Red flags

- Deletions dated after the letter of claim: Example 3's timeline.
- Hold notices silent on former employees.
- Soft-deletion windows expiring during correspondence: Example 1's day thirty.
- Inactive mailboxes absent for custodians who left mid-dispute.
- "Standard process" cited without the policy and execution records.
- OneDrive retention at platform default on a litigation-prone tenant.
- Opposing productions omitting known departed custodians without reconstruction.

When to involve a digital forensic expert

The day a relevant leaver is identified: the clocks are running and the conversion actions of §5 are the first hour's work (Example 1's restore); through preservation, where inactive mailboxes, OneDrive exports and audit harvests are verified rather than assumed; at reconstruction, where hard-deleted custodians are rebuilt from the estate with coverage measured (Example 2's 91%); and at challenge, where an opponent's leaver process is audited against the duty date and evidenced under CPR Part 35 (Example 3's records). Through **e-discovery.uk** and **cflab.uk**, deleted-custodian work runs from the same-day restore to the reconstructed footprint: and the difference between the two is usually a few days of nobody knowing the window existed.

§ 13 · COMMON QUESTIONS

Frequently asked questions

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), OneDrive 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, OneDrive 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.

§ 14 · REFERENCE

Glossary

Directory audit
Entra records of account creation, changes and deletion.

Hard deletion
Permanent removal after windows expire without a hold.

Inactive mailbox
A deleted user's mailbox preserved under hold, searchable without a user.

Leaver process
The routine that de-licenses and deletes departed users' accounts.

Litigation-pause step
The leaver-process control exempting relevant custodians.

OneDrive retention
The post-deletion period a user's files are kept.

Reconstruction coverage
The measured proportion of a lost custodian rebuilt from the estate.

Restore-hold-delete
The sequence converting a soft-deleted user into an inactive mailbox.

Soft deletion
The reversible state after user deletion (currently 30 days).

Unified audit log
Microsoft 365's cross-service record of user and admin actions.

Sources and authoritative references

The deleted-account disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (inactive mailboxes, holds and deleted-custodian collection as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- cflab.uk, digital forensics services (custodian reconstruction, device recovery, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft Learn, inactive mailboxes: learn.microsoft.com, inactive mailboxes · Restore a deleted user: learn.microsoft.com, restore user · OneDrive retention for deleted users: learn.microsoft.com, OneDrive retention
- PD 57AD (preservation duty, including former employees): justice.gov.uk, PD 57AD · CPR Part 31 (r.31.17): justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- ICO, UK GDPR guidance (retention and legal claims): ico.org.uk · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Deleted-custodian work at **e-discovery.uk** starts with the clock map: every relevant leaver's account state established the same day, soft-deleted users restored, holds converting mailboxes to inactive, OneDrive retention extended and exported with versions, and the audit and directory layer harvested before its own retention runs (Example 1's four actions, in order). Where the clocks have run, the laboratory side rebuilds the custodian from counterparts, shared stores, other members' Teams copies, backups and devices, with coverage measured and gaps stated (Example 2's method), and audits opposing leaver processes against the duty date for the applications Example 3 describes, reporting under CPR Part 35. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a relevant person left within the last month, the restore window may still be open: today's call is worth a complete custodian.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace