



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Collecting Evidence from Google Workspace

Gmail, Drive, Shared Drives, Chat, Meet and Admin Data: the Other Tenant, Mapped

Half of UK business runs on Google Workspace, and disputes involving it inherit a platform with its own geography: Gmail's label-based mailboxes, Drive's ownership model and Shared Drives, Docs' continuous revision histories, Chat's spaces and retention behaviours, Meet's recordings, and an admin layer whose audit reports and Takeout exports differ in reach and fidelity from anything in the Microsoft world. The instincts built across this series transfer: race the clocks, hold before you argue, collect structures not just files, walk the counterparts: but the mechanics are Google's own. This guide maps the estate service by service, sets out the preservation moves and their deadlines, compares the collection routes, and works through the disputes: deleted mail, revision-history authorship, Shared Drive membership, leaver accounts: that Workspace matters actually turn on.

© Estimated reading time: 27 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. Google Workspace collection runs alongside its Microsoft 365 practice: Vault preservation and export, Drive and revision-history analysis, Gmail authenticity work, and the admin-report chronologies that mirror guide 57's audit method on Google's estate. Its eDiscovery arm, **e-discovery.uk**, processes Workspace collections at disclosure scale.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

WORKSPACE & VAULT COLLECTION

DRIVE & REVISION ANALYSIS

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: same instincts, different geography
- 03 The estate map: service by service
- 04 Preservation: holds, retention and the leaver licence trap
- 05 Collection routes: Vault, Takeout, API and their fidelity
- 06 Drive evidence: ownership, Shared Drives and revision histories
- 07 The admin layer: audit reports and account records
- 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

Executive summary

THE HEADLINE POINT: THE M365 DISCIPLINES TRANSFER WHOLE; ONLY THE MECHANICS ARE GOOGLE'S

Everything this series built for Microsoft 365 has a Workspace equivalent, and the week-one playbook translates line for line. **Holds:** Google Vault places litigation holds over Gmail, Drive (including Shared Drives), Chat and Meet recordings: preserving content through user deletion and retention expiry, with the hold's placement date again the governing fact for everything recoverable. **Retention:** Vault retention rules and default behaviours set the clocks: Chat histories can run short where history is off, Drive trash empties on a rolling window (about 30 days), and deleted accounts follow a grace-period pipeline (20 days for full restore, with data transfer options at deletion): the lever trap wears Google colours. **Audit:** the admin console's audit and investigation reports record sign-ins, Drive activity (access, download, sharing, deletion), admin actions and Vault operations themselves: licence- and edition-bound in reach and retention, and subject to the same export-first-argue-later rule guide 57 made mandatory. **Collection:** Vault export is the compliance route (scope-driven, format-constrained, metadata reports alongside); API-based collection preserves structures Vault flattens (Drive revision histories as series, Chat threading, label taxonomies); Takeout is the user-level export whose convenience conceals fidelity costs: the guide 52 framework: trust, structures, downstream: chooses among them here exactly as there. The distinctly Google fact to internalise: **Docs, Sheets and Slides are not files with versions but continuously revised documents** whose revision histories are the primary record: named, timestamped, fine-grained: making Drive the richest drafting-history source in either ecosystem, and making any collection that exports only current-state PDFs an evidential amputation.

- **Vault holds on day one:** custodians, Shared Drives, Chat spaces and Meet recordings named: the clocks stop where the hold reaches, and nowhere else.
- **The lever pipeline is shorter than memory:** deleted accounts are fully restorable for 20 days: suspension (licence retained) instead of deletion is the standing advice, and the transfer-on-deletion option is the fallback.
- **Revision histories are the crown jewels:** native Docs/Sheets/Slides carry per-edit records with named editors: collected as series via the structural route wherever drafting or timing is in issue.
- **Chat history settings decide what exists:** history-off spaces retain almost nothing: the setting's state and change history are the first facts in any Chat dispute.
- **Admin reports are the guide 57 diary here:** Drive activity, sign-ins, admin and Vault operations: export the full window in week one, and request the opponent's expressly.

The problem in plain English: same instincts, different geography

Lawyers who learned their cloud disclosure on Microsoft estates arrive in Workspace with the right instincts and the wrong map. Gmail has no folders: it has labels, and one message wearing three labels is one message, not three: deduplication and scope both change. Drive has no drive letters: it has ownership, and a departing user's "My Drive" files can orphan differently from a Shared Drive's, whose membership model is the possibility map. Docs are not Word files: the .docx you export is a rendering of a living revision stream, and the stream is the evidence. Chat is not Teams: history toggles change what is kept at all. None of this is harder; all of it is different, and the cost of assuming equivalence is scope that misses, requests that misname, and productions that flatten.

This guide is the translation layer: each M365-block discipline restated in Google's terms, with the platform-specific traps: the 30-day trash, the 20-day account window, the history-off space, the current-state-only export: flagged where they bite.

§ 0 3 · THE MAP

The estate map: service by service

SERVICE	WHAT IT HOLDS · WHAT MATTERS EVIDENTIALLY
Gmail	Label-based mailboxes (one message, many labels); conversation threading; drafts; settings including filters, forwarding and delegation (the guide 53 configuration exhibit, Google edition); full headers with authentication results for authenticity work.
Drive (My Drive)	User-owned files; native Docs/Sheets/Slides with revision histories; uploaded files with version stacks; sharing per item (people, link types); trash with ~30-day auto-purge; activity records per file.
Shared Drives	Team-owned estates: membership roles as the permission model; files survive member departure (the anti-orphaning design); their own trash and manager controls: guide 55's site, in Google form.
Chat	Direct messages and spaces; history on/off per conversation type and policy; Vault reach where history is on; attachments via Drive: the fastest clocks in this tenant.
Meet	Recordings to organiser's Drive; attendance reports (edition-dependent); calendar linkage: the five-part assembly of guide 56, Google parts.
Calendar / Contacts / Keep / Sites	The perimeter services disputes forget: event histories, guest lists, notes and internal sites: named in scope when the issues touch them.
Admin console	Audit and investigation reports; user and licence management; Vault operations log; data transfer and export tooling: the governance and diary layer.

Preservation: holds, retention and the leaver licence trap

- **Vault holds, scoped in writing:** per custodian and per Shared Drive, covering Gmail, Drive, Chat (history-on content) and Meet recordings: placed day one, documented with dates, because the hold-versus-deletion race decides recoverability here exactly as in guide 53.
- **Retention rules read before relied on:** Vault's default and custom rules (what they cover, since when, and their change history): the paperwork behind every "expired" claim, requested from opponents per guide 57's compliance-events logic.
- **The trash clocks:** Drive trash auto-purges around 30 days; Gmail's deleted mail follows its own window: unheld deletions are genuinely leaving on schedule while scoping letters circulate.
- **The leaver trap, Google edition:** deleting an account starts a short full-restore window (about 20 days) after which content is gone unless a hold, retention rule or transfer preserved it: the standing instruction is suspend, do not delete: and where deletion already happened, the transfer and Vault questions are asked in hours, not weeks.
- **Chat history settings frozen:** the on/off state, its policy defaults and any changes: preserved and exhibited, because in Chat the setting is the retention regime.

Collection routes: Vault, Takeout, API and their fidelity

- **Vault export (the compliance route):** scope by custodian, term and date; exports mail (with metadata files), Drive contents, Chat and Meet material: the defensible default, whose limits are structural: native revision histories are not exported as series, and format choices flatten living documents into snapshots.
- **API-based collection (the structural route):** Drive revision series with editor attribution, activity records, Chat structures, label taxonomies: guide 52's case for structure, at its strongest in the ecosystem where the crown-jewel evidence is a revision stream.
- **Takeout (the user route):** convenient, user-initiated, and evidentially thin: formats vary, metadata is partial, and the operator is the custodian: guide 51's PST warning wearing Google colours: acceptable only with eyes open and corroboration planned.
- **The choose-by-purpose rule:** Vault for defensible bulk; API for the documents and conversations in issue; never Takeout for the contested core: and the specification, manifests and hashes disciplines of this series apply unchanged.
- **Fidelity documented:** whichever route runs, the report states what the export preserves and flattens: the honesty that survives the other side's expert.

Drive evidence: ownership, Shared Drives and revision histories

- **Revision histories as primary record:** native documents carry per-edit revisions with editors and timestamps: differenced into drafting chronologies (guide 50's method), deciding authorship and timing disputes with a granularity Office files rarely match; named-version markers and revision pruning behaviours are read alongside.
- **Ownership determines survival:** My Drive files ride their owner's account fate; Shared Drive files ride the drive's: the first question about any disputed file is which regime owned it on the relevant dates.
- **Membership is the possibility map:** Shared Drive roles (manager through viewer) enumerate the audience: exported as data, reconstructed as at dates from admin reports: guide 55's discipline, simpler model.
- **Sharing states and activity:** per-item shares and link types, plus Drive activity records (views, edits, downloads, shares, deletions by account): the event stream guide 54 built exfiltration and access findings on, available here through the admin layer.
- **Orphan and transfer archaeology:** departed owners, transferred files and the artefacts each leaves: the provenance questions asked before anyone argues from a file's current home.

The admin layer: audit reports and account records

- **The report families:** login/sign-in (with context), Drive activity, admin actions, Vault operations, email log search (delivery-level records), and the investigation tool on higher editions: the guide 57 map, Google names.
- **Windows are edition-bound:** report retention runs to months and varies by edition and report type: the full-window export in week one is the same non-negotiable, for the same unforgiving reason.
- **Vault operations are logged:** holds created and released, exports run, retention rules changed: the litigation-conduct record, requested from opponents in every retention dispute (Example 2 of guide 57 translates directly).
- **Attribution stays layered:** account events plus sign-in context plus device artefacts plus conduct: the join is ecosystem-independent, and shared-credential alternatives are canvassed here as everywhere.
- **Independence where admins are interested:** the export supervised or performed independently when console holders sit inside the dispute's perimeter: guide 52's operator logic, unchanged.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine Workspace in isolation. The estate's evidence coexists in: device-side sync (Drive for desktop mirrors and caches: guide 54's census logic; offline mail in clients); mobile apps (Gmail, Drive and Chat caches); counterpart tenants and providers (every external message and share); personal Google accounts (the consumer twin one click away: guide 69's territory, flagged wherever client logs show dual sign-in); third-party backup platforms covering Workspace; the admin/audit layer; browser artefacts (web-first ecosystems leave rich browser evidence: histories, cached documents, session traces: guides 41 and 125); and the paper-and-export trail of shared and circulated copies. When Workspace's own windows have run: devices, counterparts and backups carry the recovery, and the admin export frames what existed.

EVIDENCE	WORKSPACE (VAULT REACH)	DEVICE SYNC / CACHES	COUNTERPART TENANTS	ADMIN / AUDIT REPORTS	BACKUP / EXPORT LAYER	DELETED / RECOVERABLE
Mail	Y, per hold + retention	Client stores, offline caches	Y for external mail	Email log search: delivery facts	Y where deployed	Hold beats trash clocks
Drive files	Y + revision streams	Desktop mirrors: as last synced	Recipient copies	Activity events	Point-in-time sets	~30-day trash; hold suspends
Drafting history	Y: revisions (API route)	Cached renderings	As-shared generations	Edit events	Generational states	Pruning behaviours noted
Chat	History-on content only	App caches: sometimes	External participants' estates	Message events (edition-bound)	Where covered	History-off: little anywhere
Deleted accounts	20-day restore; holds persist	Mirrors survive account death	Their copies unaffected	Deletion events	Pre-deletion sets	The suspension advice exists for this row

Fallback strategy in one line: when Vault's reach ends, the desktop mirror, the counterpart tenant and the backup set are the walk: and for Chat with history off, start from the participants, because the tenant kept almost nothing.

Worked examples

EXAMPLE 1 · THE REVISION STREAM THAT DATED THE DEAL MEMO

A joint-venture claim turned on whether a deal memo recording generous terms was drafted before or after the relationship soured: the file's visible date said before; the defendant said fabricated after. The Doc's revision history, collected as a series via the API route, ran to 214 revisions: the memo genuinely created in the friendly period, but the two disputed clauses entered at revisions 198-203, edited by the claimant's account across ninety minutes on a date fourteen weeks later: the evening after the first hostile letter. Named-version markers showed a "final" designation applied the same night. The stream did what no metadata field could: dated each sentence. The clauses fell; the rest of the memo stood; and both sides' experts agreed on the chronology because the record left nothing to disagree about.

EXAMPLE 2 · THE HISTORY-OFF SPACE AND THE TWO PHONES

A partnership dispute alleged a campaign of pressure conducted in a Google Chat space; the respondent produced the space: empty, history off, "nothing was retained, nothing to disclose". The setting was genuine: Vault held nothing: but the architecture walk delivered anyway: both complainants' phones, imaged, carried Chat app caches with substantial message content from the relevant weeks; the admin reports (exported in week one) showed the space's history setting toggled off by its manager two days after a grievance was lodged: an event with an account and a timestamp: and one participant's contemporaneous screenshots, weak alone, corroborated the cache content precisely. The tribunal treated the toggle as conduct and the caches as content. History off had governed the tenant; it had never governed the phones.

EXAMPLE 3 · THE DELETED ACCOUNT INSIDE THE 20 DAYS

A director resigned amid fraud allegations on a Thursday; by Monday an over-tidy IT contractor had deleted his account: My Drive, Gmail, the lot: and the client called their solicitors on day 9 believing the evidence gone. It was not, twice over: the account sat within the full-restore window and came back whole on day 10; and a Vault hold placed months earlier for an unrelated regulatory matter had independently preserved his mail through any deletion. The restored Drive's revision histories then carried the case: invoice documents whose revision streams showed systematic amount edits by his account across two years. The margin was eleven days; the lesson is the guide's standing advice: suspend, never delete: and when deletion has happened, count the days before conceding anything.

Common mistakes and technical limitations

Common mistakes

- **M365 assumptions imported wholesale:** folder-thinking in a label estate; scope that misses Shared Drives; "the mailbox" requested where labels and threads change what that means.
- **Current-state-only Drive collection:** the revision streams: Example 1's whole case: flattened into PDFs.
- **Chat scoped without the settings:** history state and its change log unexamined: Example 2's toggle missed.
- **Leaver accounts deleted "to save licences":** Example 3's near-miss, run past day 20.
- **Takeout as strategy:** the custodian-operated export standing where Vault or API collection should.
- **Admin reports unexported:** guide 57's cardinal sin, Google edition: the windows lapse identically.
- **Vault operations never requested:** opponents' hold and retention conduct unexamined in "expired" disputes.
- **Personal-account signals ignored:** the consumer Google account in the sync client, unflagged and unpursued.

Technical limitations

- **Vault reach is bounded:** history-off Chat, some service data and perimeter apps sit outside it: coverage stated per matter.
- **Export fidelity varies by route:** revision series, labels and threading survive by specification: the standing guide 52 caveat.
- **Report windows are edition-bound:** audit reach differs by edition and report family: promised only after the licence facts are known.
- **Revision streams have platform behaviours:** pruning and consolidation of old revisions occur: the report states granularity honestly per document.
- **Attribution remains layered:** the ecosystem changes; the join does not.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Edition and licence facts; Vault coverage; audit-report windows: established today, with the full-window export run?
- Custodian map: My Drives, Shared Drives, Chat spaces (and their history settings), Meet recordings: and any leavers anywhere in the deletion pipeline?
- Retention rules and their change history; any personal-account sync signals on corporate devices?

Ask your opponent

- Please confirm Vault holds (scope and placement dates) for [custodians and Shared Drives], the retention rules in force with change history, and that no account deletion, transfer or licence change affecting them has occurred since [date].
- Please produce the Drive revision histories as series for [documents], the Chat history settings and their audit trail for [spaces], and the admin audit reports (login, Drive, admin, Vault operations) for [period].
- Please state the collection route(s) used for Workspace disclosure and what each preserves of labels, threading and revision structures.

Ask your eDiscovery / forensic provider

- Which sources need the API route here, and what will Vault export flatten if used alone?
- What do the revision streams show for the documents in issue: and at what granularity, given pruning?
- What does the admin-report export establish before its windows roll?

SUGGESTED WORDING · WORKSPACE LIMB FOR THE WEEK-ONE INSTRUCTION

"With immediate effect: (1) place Google Vault litigation holds over the custodians and Shared Drives at Schedule A, covering Gmail, Drive, Chat and Meet recordings, and confirm placement dates; (2) make no deletion, suspension-to-deletion, transfer or licence change affecting any listed account, suspending rather than deleting any leaver; (3) preserve and exhibit current retention rules and Chat history settings with their change histories, making no changes; (4) export and preserve the admin audit reports (login, Drive activity, admin actions, Vault operations, email log search) for the full available window, repeating at [interval]; and (5) confirm each step in writing with the responsible role. Collection routes will be specified separately per source in accordance with the matters in issue."

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

The Workspace checklist

- ☐ Vault holds placed day one: custodians, Shared Drives, Chat, Meet: dates documented
- ☐ Leavers suspended, never deleted; any deleted account's 20-day clock counted immediately
- ☐ Admin-report full-window export run in week one; repeats diarised
- ☐ Chat history settings and change logs preserved and exhibited
- ☐ Retention rules and change history obtained: yours and, by request, theirs
- ☐ Revision histories collected as series for documents in issue (API route)
- ☐ Shared Drive membership exported as data; as-at reconstruction planned
- ☐ Labels, threading and structures specified in every export
- ☐ Device census run where sync clients touch the issues; personal-account signals escalated
- ☐ Vault operations log requested in every "expired" dispute

Red flags

- A leaver account deleted after the duty arose.
- Chat history toggled off near a key date.
- Drive disclosure as current-state exports where revisions exist.
- Takeout productions for contested custodians.
- "Expired under retention" with no rule paperwork or Vault-operations disclosure.
- Admin-report windows allowed to lapse after a preservation letter.
- A consumer Google account signed into the corporate sync client.

When to involve a digital forensic expert

At week one, where holds, the leaver clock and the report export are won or lost; at route selection, where Vault's reach and the API's structures are matched to the issues; at revision-stream analysis, where Example 1's sentence-level chronologies are built and defended under CPR Part 35; and whenever the tenant's answer is "nothing retained": Example 2's walk through caches, counterparts and toggle events is laboratory work, and Example 3's day-counting is the difference between recovery and eulogy. Through **e-discovery.uk**, Workspace collections are processed with labels, threads and revisions intact into review.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is Google Vault the same kind of thing as Microsoft Purview?

Functionally sibling: holds, retention, search, export over the tenant's services: and the same jurisprudence of use applies: defensible for scope and bulk, structurally limited at the edges (revision series, history-off Chat), operator-dependent for trust. Guide 52's three questions: trust, structures, downstream: choose between Vault and independent routes exactly as they choose around Purview; guide 59 examines Vault's capabilities and limits in full.

Can deleted Gmail be recovered?

Run the layer walk: user trash within its window; Vault-held mail regardless of deletion (the hold date governs); retention-rule coverage; then the architecture: device mail caches, counterpart recipients, backup platforms. Google-specific wrinkle: labels mean "deleted from Inbox" often just means relabelled: the message may simply be elsewhere in the mailbox. The four facts of guide 53 translate: hold status and date, retention rules, window position.

How reliable are Google Docs revision histories as evidence?

Highly, within stated limits: platform-maintained, editor-attributed, timestamped, and effectively impossible for users to falsify retrospectively: Example 1's decisiveness is typical. The caveats are granularity (old revisions can be consolidated: the stream's resolution is stated per document), shared-credential attribution (the join, as ever) and collection route (streams survive as series only via the structural route). Collected properly, they are among the strongest drafting evidence in either ecosystem.

The space had history off. Is the chat genuinely gone?

From the tenant, very largely yes: that is what the setting does, and Vault cannot reach what was never kept. But Example 2 is the standard answer: participants' device caches, the other organisation in external conversations, screenshots and forwards as corroboration, and the setting's own change history as potential conduct evidence. "History off" ends the tenant inquiry and starts the architecture one.

What happens to a departed employee's My Drive files?

They ride the account: suspension preserves everything; deletion starts the 20-day restore clock, with an option at deletion to transfer Drive ownership to another user (which preserves content but rewrites provenance: the transfer is documented and stated). Shared Drive files are unaffected by member departure: the design reason disputes increasingly turn on which regime owned the file. The advice is unchanging: suspend, decide later.

We are a Microsoft firm facing a Google-estate opponent. What do we ask first?

Three requests, all in this guide's §11: hold scope and dates plus retention rules with change history (the preservation position); the admin audit reports for the period (the diary, before its windows roll); and route-and-fidelity confirmation for their collection (what their exports preserved of labels, threads and revisions). The answers map their estate and their conduct at once: and nothing in them requires you to run Workspace yourself.

§ 1 4 · REFERENCE

Glossary

Admin reports

The console's audit families: login, Drive, admin, Vault operations; the diary layer.

History setting

Chat's per-space retention switch; in Chat, the regime itself.

Labels

Gmail's non-exclusive message taxonomy; folder-thinking's replacement.

My Drive

User-owned storage riding the account's fate.

Revision stream

A native document's per-edit history; the primary drafting record.

Shared Drive

Team-owned storage with role-based membership; survives departures.

Suspension

The lever state that preserves everything; the alternative to the 20-day clock.

Takeout

User-level export; convenient, evidentially thin.

Transfer (on deletion)

Ownership handover preserving content, rewriting provenance.

Vault

Workspace's hold, retention, search and export service; guide 59's subject.

Sources and authoritative references

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

- cflab.uk, digital forensics services (Workspace collection, revision-stream analysis, Gmail authenticity, admin-report chronologies, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation, Phase 03 · Collection and Phase 04 · Processing (Vault and API collection; labels, threads and revisions into review): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Google documentation: Vault help and admin audit reports: support.google.com/vault · support.google.com, [audit and investigation](https://support.google.com/audit-and-investigation) · account deletion and restoration: support.google.com, [restore deleted user](https://support.google.com/restore-deleted-user)
- PD 57AD and CPR Part 35: justice.gov.uk, [PD 57AD](https://justice.gov.uk) · justice.gov.uk, [Part 35](https://justice.gov.uk)
- ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about Google Workspace evidence as at August 2026. Platform behaviour, windows, editions and defaults change on Google's schedule and vary by tenant and configuration; verify current behaviour and entitlements in the matter at hand. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

The laboratory runs Workspace matters on the translated playbook: Vault holds and the leaver-clock triage in day one; admin-report exports before the windows roll; route selection per source (Vault for bulk, API for the revision streams and structures the issues demand); and the analyses this guide's examples model: sentence-dating from revision series, history-off rescues from caches and counterparts, deleted-account recoveries with the days counted. Cross-ecosystem matters: Microsoft one side, Google the other: are routine, with the disciplines mapped between estates rather than reinvented. Reporting is CPR Part 35 with reach, granularity and windows stated; processing through **e-discovery.uk** keeps labels, threads and revisions alive into review. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if an account has already been deleted, the first question is the date, today.



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