COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Personal Email Accounts in Disclosure

Gmail, Hotmail and the Business That Left the Building

Somewhere in almost every commercial dispute sits a personal email account doing corporate work: the director who forwards board papers to his Gmail, the salesperson negotiating from her Hotmail, the founder whose Yahoo predates the company and never stopped, the deliberate off-books channel chosen precisely because the company's servers do not see it. Personal accounts are where corporate control ends and the hard questions begin: whether their contents are disclosable at all, how to search an account the party's solicitors cannot log into, what self-collection by the account holder is worth and how to police it, and what forwarding rules, sign-in logs and device caches reveal when the account holder says there is nothing to see. This guide covers the control analysis for personal webmail, the collection routes from supervised self-collection to independent-examiner protocols, the forensic periphery that checks the account holder's account of their account, and the conduct significance of business deliberately routed around the corporate record.

⏱ Estimated reading time: 26 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. Personal-account collection is core casework: supervised and examiner-led webmail acquisition, forwarding-rule and sign-in-log analysis, device-cache recovery of webmail the account no longer shows, and the completeness verification that self-collections require. Its eDiscovery arm, **e-discovery.uk**, brings the personal slice into the corporate review estate.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | WEBMAIL & PERSONAL-ACCOUNT COLLECTION | SELF-COLLECTION VERIFICATION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: THE BUSINESS CONTENT OF A PERSONAL ACCOUNT IS USUALLY DISCLOSABLE, THE ACCOUNT HOLDER USUALLY COLLECTS IT, AND THE FORENSIC PERIPHERY CHECKS THEIR WORK

Personal email in disclosure runs on three findings this series has been building toward. **First, disclosability:** where a custodian conducted relevant business through Gmail, Hotmail, Yahoo or any personal account, the business documents in it are disclosable: for a party custodian, directly; for employee custodians, through the control analysis of guide 68 §3 (employment duties, policy consents, practical ability to require production): with the courts long past being impressed by "but it's my personal account" as an answer to business content: the account is personal; the deal correspondence in it is not. **Second, the collection asymmetry:** unlike the corporate tenancy, nobody but the account holder (or their delegate) can lawfully log in: so collection runs through them: ranging from **supervised self-collection** (the custodian searches under written protocols, with terms, scope and export method specified) through **solicitor-supervised collection** to the **independent-examiner route** (credentials provided to the laboratory under protocol, full-account acquisition, filtering per guide 68 §5's intermediary model): the route escalating with the stakes, the custodian's alignment, and the case's history of candour. **Third, the verification layer:** self-collection is testimony in export form: it is checked, not trusted: the account's own machinery: sign-in and activity logs, folder structures, forwarding rules and their histories, filter configurations, deletion behaviours, linked-device lists: plus the periphery outside it: device caches and mail-client stores holding messages the account no longer shows, counterpart mailboxes holding the other end, and the corporate estate's forwarding trail (the auto-forward that created the shadow archive is itself logged corporate-side, per guide 57): the machinery that catches both the innocent gap and the curated production. Above all this sits the conduct layer of §6: business deliberately routed to personal accounts to evade the corporate record: the discovery of which reframes cases: the routing's chronology (when did the personal channel start, relative to what), its selectivity (which topics went off-books), and its aftermath (deletions, account closures) all pleading intent: because in personal-account matters, where the email went is often as probative as what it said.

- **Business content is disclosable wherever it lives:** the personal-account objection goes to collection method, not to the duty.
- **Collection runs through the holder:** the route: self, supervised or examiner-led: is chosen deliberately and escalated on the facts.
- **Self-collection is verified:** account logs, rules, devices and counterparts check the export: trust is a finding, not a starting point.
- **The forwarding trail is corporate-side evidence:** auto-forwards and manual forwards to personal accounts are logged where the company can see them: the census starts there.
- **Off-books routing is conduct:** the deliberate personal channel, dated and mapped, is frequently the case's most eloquent fact.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the account the company cannot open

The corporate mailbox answers to the company: holds, searches and exports run administratively, per guides 51-53. The personal account answers to one person: the provider's contract is with them, the password is theirs, and neither employer nor opponent nor court can simply log in. Yet the business that matters may be inside: forwarded board papers, side-channel negotiations, the candid versions of sanitised corporate threads. Disclosure law resolves the standoff by obligation rather than access: the account holder must search and produce: which converts a technical problem into a candour problem: the quality of disclosure now depends on the diligence and honesty of the person with the most at stake.

The practitioner's response is the architecture of this guide: choose the collection route to match the custodian and the stakes; wrap even willing self-collection in protocols that specify terms, scope and method; and always run the verification layer, because the account's own logs and the estate around it: devices, counterparts, corporate forwarding records: let the diligent be confirmed and the curated be caught. The personal account cannot be opened from outside; it can be checked from outside: and the checking is where these matters are won.

§ 0 3 · THE DUTY

Control and disclosability of personal accounts

- **Party custodians:** a party's own personal account holding relevant documents is squarely within the disclosure duty: searched per the DRD/order, addressed in the disclosure statement, with "personal" limiting nothing but the search's scope of relevance.
- **Employee custodians:** guide 68 §3's control analysis transfers: employment duties, policies and practical ability commonly give the employer control of the business content: the disclosure statement addresses personal accounts custodian by custodian in any case pleaded on off-channel dealings.
- **Directors and officers:** the strongest case: fiduciary duties and service agreements make business correspondence in personal accounts company-reachable in most commercial disputes: authority has proceeded on exactly this footing.
- **Leavers and third parties:** the weakening-control problem of guide 68 §7: surviving duties, joinder, and third-party disclosure under CPR 31.17 against the account holder: with the corporate forwarding trail often proving what the unreachable account contains.
- **Scope discipline:** the duty reaches relevant business content, not the account: search design (terms, dates, participants) confines the intrusion, and §7's protections govern the rest.

§ 0 4 · THE ROUTES

Collection routes: from self-collection to examiner protocols

- **Supervised self-collection:** the custodian searches their own account under a written protocol: specified terms and date ranges, all-folders scope (including sent, archive, bins), native export where the provider supports it (takeout-style archives preferred over forwarding), and a signed statement of method and completeness: the proportionate default for aligned custodians and modest stakes.
- **Solicitor-supervised collection:** the searches run in the solicitor's presence or via screen-share, contemporaneously recorded: the middle rung when stakes rise or first productions disappointed.
- **Examiner-led acquisition:** credentials to the independent laboratory under a guide 68 §11-style protocol: full-account collection by API or archive export, filtering by the intermediary, personal material never reaching the parties: the route for central custodians, contested candour, or forensic questions (deletion, tampering) that self-collection cannot answer.
- **Provider-archive exports:** the personal-account cousin of guide 67 §4: Google Takeout and equivalents produce structured, metadata-bearing archives: the preferred acquisition format at every rung, because headers and internal dates survive intact for guide 53-style verification.
- **Route escalation is evidence-driven:** gaps found by §5's verification justify the next rung: and the escalation history itself: offers made, protections offered, cooperation declined: builds the record for orders and inferences.

§ 0 5 · CHECKING THE WORK

Verifying completeness: the forensic periphery

- **The account's own machinery:** webmail providers log sign-ins (times, devices, locations), expose folder structures and counts, record forwarding rules and filters with their histories, and list connected apps and devices: the self-audit layer a protocol can require the custodian to export alongside the mail.
- **Deletion behaviour per provider:** bins with time-limited retention, archive-versus-delete distinctions, provider-side recovery windows: known per platform and checked against the production's gaps: a thread that "never existed" versus one deleted last Tuesday are different findings.
- **Device caches and clients:** phones and computers that synced the account hold mail-client stores and webmail caches: messages the account no longer shows, recovered per guides 61 and 41-42: the layer that has repeatedly outed curated self-collections.
- **Counterpart mailboxes:** every relevant thread has other ends: corporate mailboxes (collected per guide 53) and other parties' accounts: the convergence standard applied to the self-collection's claims.
- **The corporate forwarding trail:** message-trace and audit logs (guide 57) record what was forwarded to the personal account and when: the company can often prove the shadow archive's contents into existence from its own records before the account holder produces a thing.

§ 0 6 · OFF THE BOOKS

Deliberate off-books channels: conduct and consequences

- **The routing is datable:** when the personal channel began for the relevant topic: first off-books message, auto-forward creation date (logged corporate-side), the migration invitation ("use my gmail for this"): dated against the dispute's chronology exactly as guide 64 §6 dates Signal migrations.
- **Selectivity argues content:** routine business on corporate mail, the disputed topic on Gmail: the pattern mapped across the estate pleads awareness that the topic needed hiding.
- **Aftermath compounds:** deletions from the personal account post-duty, account closures, forwarding rules removed: each logged or datable, each joining the spoliation analysis this series builds everywhere.
- **Regulatory shadows:** off-channel business communication is an enforcement theme in regulated sectors: the same conduct that prejudices the litigation may be a standalone compliance failure: advice to regulated clients says so.
- **The innocent version exists:** founders' legacy accounts, IT outages, habit: the explanation is tested, not assumed either way: chronology, selectivity and aftermath separate the sloppy from the strategic.

§ 0 7 · RIGHTS

Privacy, mixed content and the account holder's rights

- **The account is a life:** two decades of correspondence, family, health, finances: the intrusion is real and the protections are the price of the order: search-term confinement, examiner filtering, review protocols that keep irrelevant personal material from the parties.
- **UK GDPR discipline:** the guide 68 §6 analysis transfers: lawful basis, minimisation by design, transparency through the protocol, third-party correspondents' data handled with care.
- **Privilege wrinkles:** personal accounts hold the custodian's own legal advice (matrimonial, personal disputes): flagged in protocols, filtered by the intermediary, never fished from by the instructing party.
- **Proportionality shapes scope:** the account's centrality moves the dial: a director's dedicated deal-channel justifies full acquisition; a peripheral custodian's incidental forwards justify targeted terms: reasons recorded, per the series' standing method.
- **Cooperation is purchasable:** Example 1 of guide 68's lesson transfers whole: protections offered early convert refusals into protocols: the demand that respects the life inside the account is the demand that gets answered.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the webmail login page is one door to an estate with several. Personal-account evidence also lives in: the provider's structured archive exports (Takeout-class, metadata intact); mail clients and caches on every device that synced the account (phones, laptops, tablets: the offline copies); device backups capturing those stores (guide 65's lineages); the corporate estate's forwarding and message-trace records proving traffic into the account; counterpart mailboxes holding every thread's other end; the account's own logs (sign-ins, rules, filters, connected devices): exportable and demandable; linked accounts (recovery addresses, aliases, secondary accounts discovered from headers and sign-in trails); and provider-side records behind legal process for the attribution layer. When the account holder stonewalls, this periphery is the case: the corporate trail proves what went in; the counterparts prove what came out; the devices prove what was seen; and the stonewalling, dated, proves itself.

EVIDENCE	WEBMAIL ACCOUNT (HOLDER-MEDIATED)	PROVIDER ARCHIVE EXPORT	DEVICE CLIENTS & CACHES	CORPORATE FORWARDING TRAIL	COUNTERPART MAILBOXES	DELETED / RECOVERABLE
Business threads	Y: per route and candour	Y: structured, headers intact	Synced copies, offline stores	Inbound traffic logged	Y: the other ends	Bins, windows, caches, counterparts
Forwarding / rules history	Settings + histories	Included in some exports	n/a	Rule creation logged corporate-side	Received-header trail	Logs outlive rules
Sign-in / device history	Account activity logs	Y in archive data	Session artefacts	n/a	n/a	The attribution layer
Deletions	Bin contents, window-bound	Pre-deletion archives	Cache survivals	Inbound proof of existence	Their intact copy	Multi-layer, per provider
Linked / secondary accounts	Recovery + alias settings	Account records	Configured clients reveal them	Forward destinations logged	Headers reveal them	Discovered, then the cycle repeats

Fallback strategy in one line: prove the inflow from the corporate trail, the content from counterparts and devices, the account's behaviour from its own logs: and let the holder's production be the confirmation, not the foundation.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE AUTO-FORWARD THAT INDEXED ITSELF

A procurement manager denied any relevant material in his Gmail: "I never use it for work". The corporate estate answered first: message-trace logs showed an auto-forward rule from his work mailbox to the Gmail address, created three years earlier, and 4,100 messages forwarded: including every tender document in the disputed award's window. The rule's creation was logged; its targets were logged; the company could list what his Gmail had received without opening it. Faced with the index, the examiner-led route was agreed by consent: the acquisition matched the trace almost perfectly: and the eleven messages present in the trace but absent from the account, all deleted in one session two days after the letter of claim, carried the case's conduct findings by themselves.

EXAMPLE 2 · THE SELF-COLLECTION THE SENT FOLDER BETRAYED

A respondent director self-collected his Hotmail under protocol and produced forty-eight messages: nothing damaging. The verification layer ran anyway: his production contained inbound messages whose replies: quoted in later counterpart threads: never appeared; the counterpart collection held nine of his sent messages absent from his production; and the protocol's required settings export showed his search had excluded the sent folder entirely: per his statement, "an oversight". The re-collection under solicitor supervision produced the sent folder: sixty-two further responsive messages, including the two the claim had been missing. The tribunal accepted no bad faith on the folder point: and noted that without the counterpart convergence check, the oversight would have stood as the record.

EXAMPLE 3 · THE LEGACY YAHOO THAT PREDATED THE COMPANY

A founder's Yahoo account, older than the business, had simply never stopped: suppliers, the co-founder and two customers had used it for years alongside the corporate domain. When partnership litigation arrived, the account was a mixed archive of two decades of life and twelve years of business. The examiner-led protocol handled it: full Takeout-class acquisition to the laboratory; filtering by participant lists and the business's date range; privilege and personal filters run by the intermediary; 7,800 business messages produced into the review estate, the remaining decades never leaving the laboratory. The co-founder's challenge to completeness was answered from the account's own machinery: folder counts, no deletion events in the disputed window, sign-in history consistent: and the account that could have been the case's quagmire became its cleanest source.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **The census skipped:** personal accounts undiscovered because nobody ran the corporate forwarding trail or read the headers already in the review set.
- **"Personal" accepted as an answer:** the disclosability analysis never engaged; business content conceded to privacy rhetoric.
- **Unprotocoled self-collection:** "search your Gmail and send us anything relevant": no terms, no scope, no method statement: Example 2's sent folder, guaranteed.
- **Forward-to-solicitor exports:** collections by forwarding, destroying headers and dates that Takeout-class exports preserve: guide 53's verification made impossible by the acquisition itself.
- **Verification never run:** productions accepted without the logs, counterpart and device checks that catch the gaps.
- **Devices ignored:** the synced-client layer: the curated collection's natural enemy: never examined.
- **The routing left unpleaded:** off-books channels proven but their conduct significance: chronology, selectivity, aftermath: never developed.
- **Protections withheld:** maximal demands generating refusals that a §7 protocol would have converted.

Technical limitations

- **Provider cooperation is thin:** content from webmail providers via civil process is exceptional: the practical routes run through the holder and the periphery: expectations set accordingly.
- **Recovery windows are provider-specific:** bin retention and provider-side restoration vary and change: checked per platform, promised never.
- **Logs have horizons:** sign-in and activity histories are finite: the verification layer is richer the earlier it runs.
- **Determined curation can defeat one layer:** which is why the method uses several: account machinery, devices, counterparts, corporate trail: convergence, not any single check, is the standard.
- **Secondary accounts multiply:** aliases and further accounts discovered mid-collection restart the cycle: the census is iterative, and the protocol says so.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- The census: which custodians used personal accounts for relevant business: from the forwarding trail, header review and direct questioning?
- For each account: which route: self, supervised, examiner: fits the custodian's centrality and the case's candour history?
- Are your own side's personal accounts frozen: no deletions, no closures, no rule changes: in writing, today?

Ask your opponent

- Please identify all personal email accounts used by [custodians] for relevant business, and confirm preservation: no deletion, archiving change, rule change or account closure.
- For each account searched: please state the method (route, terms, folders, export format), and provide the account's activity, forwarding-rule and filter records for the relevant period.
- Where your disclosure statement does not address personal accounts: please explain how the duty was discharged for custodians shown by the documents to have used them.

Ask your eDiscovery / forensic provider

- What does the corporate trail already prove about traffic into the accounts?
- Which verification checks: logs, devices, counterparts: fit this production, and what do they show?
- For the examiner route: what protocol terms will this custodian and this court accept?

SUGGESTED WORDING · PERSONAL-ACCOUNT LIMB FOR THE PRESERVATION LETTER

> "Your client must immediately preserve all personal email accounts used by [custodians] for communications relevant to the issues, including: (a) all messages in all folders, including sent, archive, spam and deleted-items folders, none of which may be deleted or allowed to purge; (b) all account settings, including forwarding rules, filters and connected applications, which must not be changed; (c) the accounts themselves, which must not be closed, merged or renamed; and (d) all devices and mail clients synchronised with such accounts, which must not be wiped, deregistered or disposed of. Please identify each such account within [7] days, confirm the steps taken, and state the method by which relevant content will be searched and produced, including the export format, which should preserve full message headers."

§ 12 · QUICK CONTROL

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

The personal-account checklist

- ☐ Census run: forwarding trail, header review, custodian questioning
- ☐ Disclosability analysed per custodian; disclosure statements address it
- ☐ Route chosen per account: self, supervised, examiner: with reasons
- ☐ Protocols specify terms, folders, dates and header-preserving export
- ☐ Account machinery exported alongside mail: logs, rules, filters
- ☐ Verification layer run: counterpart convergence, device caches, corporate trail
- ☐ Off-books routing dated, mapped and pleaded where found
- ☐ Privacy protections offered early; intermediary filtering for mixed archives
- ☐ Secondary accounts pursued as discovered; census treated as iterative
- ☐ Escalation history documented for orders and inference

Red flags

- Trace-listed messages absent from the production: Example 1's eleven.
- Productions missing sent items or with reply gaps: Example 2's tell.
- Rules or accounts changed or closed post-notice.
- Collections exported by forwarding, headers destroyed.
- The disputed topic's traffic migrating to personal channels mid-chronology.
- "No relevant material" from accounts the corporate trail shows receiving it.
- Refusal of the account-machinery exports a protocol reasonably requires.

When to involve a digital forensic expert

At the census, where the corporate trail and header analysis surface the accounts; at route selection and protocol design, where the guide 68 intermediary model is adapted to webmail; at acquisition, where header-preserving exports and account-machinery capture are craft; and at verification, always: the convergence checks of §5 (Examples 1-2's machinery) are laboratory work, and the completeness opinion that survives challenge is written from them under CPR Part 35. Through **e-discovery.uk**, the personal slice is deduplicated and threaded into the corporate estate per guides 82-83, so the off-books channel is read beside the record it bypassed.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can we force an opponent to disclose their Gmail?

You can put them under a duty they must discharge: business content in personal accounts is disclosable, orders can specify search method and require the account-machinery exports, and non-compliance meets the verification layer and its consequences. What you cannot do is log in: collection runs through the holder at a route the court will calibrate: which is why §11's questions target method and records, giving the tribunal something concrete to order when the first answer disappoints.

Our custodian says the relevant messages were deleted years ago. Dead end?

Rarely a full one: provider bins and windows are checked per platform; device clients and caches hold what synced before deletion; counterpart mailboxes hold every thread's other end; the corporate trail proves inbound traffic; and archive exports predating the deletion may exist in the custodian's own backups. Plus the finding discipline: "deleted years ago" versus "deleted last month" is exactly what the verification layer distinguishes: and the difference is often the case.

Is self-collection ever defensible for important custodians?

As a first pass under a rigorous protocol, sometimes: but centrality shifts the calculus: the more the case turns on the account, the harder it is to defend a process whose completeness rests on the interested party's diligence, and the stronger the examiner-route argument becomes: protective for the custodian too, since Example 3's founder emerged with a verified clean bill no self-collection could have given him. The pragmatic rule: peripheral accounts, protocoled self-collection with verification; central accounts, the laboratory.

The personal account also holds the custodian's own privileged and intimate material. How is that handled?

By the intermediary model, which exists for exactly this: acquisition to the independent examiner, filtering by participants, terms and dates, privilege and personal filters applied before anything reaches the parties, destruction or return of the residue on defined terms: Example 3's twelve-years-of-business from twenty-years-of-life separation. The instructing party never browses the archive; the account holder's life never enters the data room; and the protocol document proves both.

We found business being run through a personal account deliberately. What do we do with that?

Develop it as §6 teaches: date the channel's start against the chronology; map its selectivity (what went off-books, what stayed on); document the aftermath (deletions, closures, rule removals); and plead the pattern: as conduct supporting inference, as spoliation where post-duty destruction followed, and in regulated contexts as a compliance dimension. The messages themselves may be recovered or not: the routing's story frequently does comparable work.

Do we need to worry about our own client's personal accounts?

First, not last: run the census on your own side at matter-open, freeze the accounts in writing, choose routes before the opponent chooses them for you, and surface any off-books history to the team early: the routing explained candidly in a witness statement reads survivably; the same facts excavated by the other side's verification layer read as Example 1. The discipline this guide aims at opponents is the discipline your own disclosure statement must survive.

§ 14 · REFERENCE

Glossary

Account machinery
The webmail account's own logs, rules, filters and device lists; the self-audit layer.

Census (accounts)
The iterative identification of personal accounts from trails, headers and questioning.

Convergence check
Counterpart-mailbox comparison against the production; Example 2's method.

Forwarding trail
Corporate-side logs of traffic into personal accounts; the census's spine.

Header-preserving export
Takeout-class acquisition keeping metadata intact; the required format.

Intermediary filtering
Examiner-applied scope, privilege and personal filters; guide 68's model on webmail.

Off-books channel
Business deliberately routed around the corporate record; §6's conduct layer.

Route escalation
Self to supervised to examiner-led, driven by stakes and verification findings.

Supervised self-collection
Holder-run searches under written protocol with method statement.

Verification layer
Logs, devices, counterparts and trails checking the production's completeness.

Sources and authoritative references

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

- cflab.uk, digital forensics services (webmail acquisition, self-collection verification, forwarding-trail analysis, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 01 · Identification, Phase 02 · Preservation and Phase 03 · Collection (account census; protocoled collection into review): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Google, Takeout data export: takeout.google.com · Microsoft, Outlook.com export options: support.microsoft.com
- PD 57AD, CPR Part 31 and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · justice.gov.uk, Part 35
- ICO, UK GDPR guidance: ico.org.uk · ISO/IEC 27037: iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Personal-account matters at the laboratory begin where §5 begins: the corporate trail and header census that prove the accounts and index their traffic before any password is asked for (Example 1's method). Routes are matched to custodians: protocoled self-collection with verification for the periphery, examiner-led acquisition with intermediary filtering for the centre (Example 3's clean separation): with header-preserving exports and account-machinery capture as standard at every rung. Productions: the opponent's and your own: meet the convergence checks that caught Example 2's sent folder; off-books routing is dated, mapped and reported as the conduct evidence it is; and completeness opinions are written under CPR Part 35 from the layers, not from trust. Through **e-discovery.uk**, the personal slice joins the corporate estate deduplicated and threaded. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a custodian's personal account is being "tidied" while routes are debated, the preservation call comes first.

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