



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

Data Exfiltration to Cloud Storage

Tracing Company Data Uploaded to Personal and Third-Party Clouds

The USB stick was the exfiltration route of the last decade; the personal cloud account is the route of this one. An employee syncs the client book to a personal OneDrive, uploads the design archive to a private Google Drive, drags the deal files into a consumer Dropbox, emails everything to a personal webmail with cloud attachments, or shares a corporate folder to an outside address. Cloud exfiltration is quieter than a USB copy and, to the untrained eye, harder to prove: the data leaves over the network, to an account the company cannot see. But it is in fact one of the best-evidenced routes in digital forensics, because it writes to both ends and several layers in between: the endpoint's sync-client databases and browser artefacts, the corporate platform's audit and sharing logs, the network's egress records, and: reachable through legal process: the personal cloud account itself. This guide sets out for UK lawyers how cloud exfiltration works, where each stage is recorded, how to prove what left and where it went, and how to reach the destination account and secure its return.

© Estimated reading time: 25 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. Cloud-exfiltration investigations are core laboratory work: the departing employee's personal-cloud sync, the shared folder to an outside address, the webmail upload: proven across endpoint, platform and network layers, quantified to a file-level manifest, and traced to the destination account through undertakings and orders, with reporting under CPR Part 35 at injunction speed.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

CLOUD-EXFILTRATION INVESTIGATION

SYNC-CLIENT & EGRESS ANALYSIS

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01	Executive summary
02	The problem in plain English: the network copy that writes to both ends
03	The routes: sync clients, browser uploads, sharing, webmail and rules
04	The endpoint record: sync databases, browser artefacts and local traces
05	The platform and network record: audit logs, sharing events and egress
06	The destination: reaching the personal cloud account through process
07	Quantification, deployment and the innocent explanation
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: CLOUD EXFILTRATION WRITES TO THE ENDPOINT, THE CORPORATE PLATFORM, THE NETWORK AND THE DESTINATION ACCOUNT: PROVE WHAT LEFT FROM THE FIRST THREE, REACH WHERE IT WENT THROUGH THE FOURTH, AND QUANTIFY TO A FILE-LEVEL MANIFEST

The routes (§3): a personal cloud sync client installed on the work machine mirroring corporate folders to the employee's account; browser uploads to a personal Drive, Dropbox or webmail; sharing a corporate document or folder to an external address; auto-forwarding rules (guide 104) carrying attachments out; and the hybrid of emailing files to personal webmail whose provider stores them in the cloud. **The endpoint (§4):** the sync client's local database lists every mirrored file with paths, sizes and sync timestamps; browser artefacts record upload sessions, destination URLs and (in histories, caches and form data) the personal account; installed-application and file-access records place the activity; and the corporate sync client's own database shows what was pulled down to be re-uploaded. **The platform and network (§5):** the corporate platform's audit log records downloads, external shares and link creation with the acting account and destination; the mail system records forwards and rules; DLP alerts, proxy and firewall logs record egress volumes and destinations; sign-in logs place the sessions. **The destination (§6):** the personal cloud account holds the received copies, with its own upload timestamps and, crucially, the material itself: reachable through preservation letters, undertakings and delivery-up or imaging orders (guide 97 §7), commonly via an independent examiner. **Quantification and deployment (§7):** the file-level manifest of what left, its sensitivity classified, the choreography timed against resignation and joining (guide 96), the innocent explanations (sanctioned personal sync, agreed home-working, role-consistent access) tested first (guide 97 Example 3): supporting springboard and confidential-information injunctions, employment proceedings, and the employer's own UK GDPR breach assessment where client personal data left.

- **Both ends record it:** the endpoint's sync database and the destination account each hold the file list: the copy the USB never had.
- **Sharing is exfiltration too:** a folder shared to an outside address moves data without a download: logged as a sharing event.
- **The network sees the volume:** proxy and DLP logs bound what left even where the endpoint is silent.
- **The destination is reachable:** the personal account is obtained through process, and holds both the manifest and the material.
- **Manifest, not adjective:** "these 4,000 files" beats "substantial confidential information" in every application.

The problem in plain English: the network copy that writes to both ends

A USB copy is a single event on a single machine, evidenced by that machine's registry and shortcut files. A cloud upload feels more elusive: the data leaves over the wire, to a service the company does not run, into an account it cannot open. Employers often assume it is therefore unprovable, and act as if the trail is cold. The assumption is exactly wrong. A cloud transfer is a transaction between two systems, each of which keeps records, mediated by a network that logs the traffic and a platform that audits the operation. The employee who uploads the client book to a personal Drive leaves the file list in the corporate machine's sync database, the download-then-upload in the browser history, the volume in the proxy log, the external share in the platform audit trail, and: at the far end: the files themselves in an account that legal process can reach.

The investigator's task is to read the near ends that the employer controls, to bound the transfer from the network layer, and to reach the far end through the machinery of guide 97: preservation letters, undertakings, delivery-up. Done in the first fortnight, before the springboard advantage matures and before the personal account can be emptied, it produces a file-level account of what left and where it went that few defendants can meet. This guide is that task, route by route and layer by layer.

The routes: sync clients, browser uploads, sharing, webmail and rules

- **Personal sync clients on work machines:** a consumer OneDrive, Google Drive or Dropbox client signed into a personal account and pointed at corporate folders: mirroring data continuously and silently: the highest-volume route, leaving a complete local manifest in the client's database.
- **Browser uploads:** dragging files into a personal cloud's web interface or a webmail's attachment picker: recorded in browser histories, upload artefacts and, often, the site's own session and form data cached locally.
- **External sharing of corporate content:** sharing a corporate document or whole folder to a personal or external address, or creating an anonymous link and taking it away: no download at all, the data reached later from outside: logged as a sharing event with the destination (guide 105 §3).
- **Webmail with cloud storage:** emailing files to a personal webmail account whose provider stores attachments in an associated cloud: the mail forward evidenced at the corporate end, the storage at the destination.
- **Rules and automation:** auto-forwarding rules (guide 104 §4) carrying every relevant message and attachment out continuously; scheduled sync jobs; connected third-party apps granted access to corporate storage and exporting on the employee's behalf: the set-and-forget routes that run after the employee has left the building.

The endpoint record: sync databases, browser artefacts and local traces

- **Sync-client databases:** each consumer sync client keeps a local database recording every file it mirrored: paths, sizes, hashes, sync timestamps and account identifiers: the single richest exfiltration artefact, naming the files, the account and the times directly (guide 97 §4).
- **Browser artefacts:** histories showing visits to personal cloud and webmail sites and upload endpoints; cached pages and session data revealing the account signed in; form-autofill and saved credentials naming the destination; download histories where files were pulled locally before upload.
- **Installed-application and account traces:** the consumer client's installation and configuration files naming the personal account; credential stores; the account switch in an application configured for corporate use: the destination account identified from the machine.
- **File-access and staging artefacts:** LNK files, jump lists and recent-file records showing the corporate documents opened and gathered; temporary copies and staging folders; the corporate sync client's database showing the files pulled down before re-upload: the harvest before the transfer.
- **The cleanup that failed:** where the employee cleaned the browser or uninstalled the client (guide 110), the sync database's residue, the corporate sync record, the credential store and the platform layer survive: the exfiltration proven from what the cleanup missed.

The platform and network record: audit logs, sharing events and egress

- **Corporate platform audit logs:** Microsoft 365 and Google Workspace record downloads, external shares, anonymous-link creation and sync activity with the acting account, item, destination and timestamp (guide 105 §3): the external share to a personal address named directly, the mass download preceding an upload quantified.
- **Mail-system records:** forwards to personal addresses, auto-forwarding rules and their creation, and attachment manifests (guide 104): the webmail and rule routes evidenced at the corporate end.
- **DLP alerts:** data-loss-prevention systems, where deployed, flag and log policy-matching transfers with the file, the destination and the action: the exfiltration the organisation's own tooling already caught.
- **Proxy, firewall and CASB logs:** web-proxy and firewall records of connections to personal cloud services with volumes and timestamps; cloud-access-security-broker logs of sanctioned and unsanctioned cloud use: the egress bounded even where the endpoint is silent, and the destination service identified from the traffic.
- **Sign-in and session context:** the corporate account's sessions (device, IP, time) around the transfers, and: where the personal account was accessed from the corporate network: its sign-ins in the network logs: the sessions joined to the person by guide 105 §7's lattice.

The destination: reaching the personal cloud account through process

- **Preservation first:** the preservation-and-undertakings letter (guide 97 §7, §11) demanding that the personal account and its contents be preserved unaltered and not deleted, downloaded further or shared: sent the moment the near-end evidence supports it, because the account can be emptied in minutes.
- **Undertakings and delivery-up:** undertakings as to non-use, non-disclosure and delivery-up sought by letter; on refusal, delivery-up and imaging orders reaching the personal account and any device holding its synced copy: commonly executed by an independent examiner who reports on the employer's material only, protecting the employee's unrelated private data.
- **What the destination holds:** the received files themselves (the material, not merely the fact of transfer), the account's own upload and access timestamps corroborating the near-end record, further sharing or downloading from the account (the second-generation spread), and the sync history to the employee's other devices: the full picture of what happened after the data left.
- **Provider records:** where the account holder does not cooperate, the cloud provider's records (upload logs, sharing history, access from the corporate network) through the provider's legal-process channels or third-party disclosure (CPR 31.17): the destination reached without the destination's help.
- **The new employer:** where the data reached a competitor, the same machinery applied to their estate (guide 97 §7): what arrived, who accessed it, and its quarantine and return: the receiving side of the transfer.

Quantification, deployment and the innocent explanation

- **The manifest:** the file-level schedule of what left: from the sync database, the platform download logs, the sharing events and the destination account, deduplicated and reconciled: Schedule 1 of the injunction and the input to the damages analysis, replacing "substantial confidential information" with a list.
- **Sensitivity classification:** the manifest classified: trade secrets, client and personal data, commercially sensitive material: driving the remedy's scope and the employer's own notification obligations where client personal data left (guide 99 §6).
- **The choreography:** the transfers timed against resignation drafting, garden-leave dates, competitor contact and joining (guide 96, guide 97 §6): the sequence that supplies intent and answers innocence.
- **The innocent-explanation pass:** tested before pleading (guide 97 §6, Example 3): sanctioned personal sync under a documented policy, agreed home-working arrangements, role-consistent access mirrored by comparable leavers, a personal client legitimately taken: the version that survives the pass is the version sworn.
- **The remedies:** springboard and confidential-information injunctions, delivery-up and certified deletion, and: where the transfer is disputed as innocent: the same evidence exonerating: with the employer's UK GDPR breach clocks running from the moment client personal data is known to have left.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: cloud exfiltration is a transfer between two estates across a network, and every stage is recorded in a layer that fails independently. The originating endpoint holds the sync database, browser artefacts and staging traces. The corporate platform holds the audit log of downloads, shares and rules. The network holds the egress record: proxy, firewall, DLP, CASB. The destination account holds the received files and its own timestamps. The provider holds the account's server-side history. The new employer's estate holds what arrived. And the behavioural layer: the employee's own messages, the search for the sync client, the competitor's job offer: supplies intent. When the employee cleaned the endpoint, the platform and network still logged the transfer; when the platform logging was thin, the network bounded the volume; when both were silent, the destination account holds the manifest and the material; and when the account was emptied, the provider's records and the corporate sync database still name the files. Redundancy across the transfer's stages is what makes cloud exfiltration, counter-intuitively, one of the best-evidenced routes there is.

QUESTION	ORIGINATING ENDPOINT	CORPORATE PLATFORM AUDIT	NETWORK EGRESS (PROXY/ DLP/CASB)	DESTINATION ACCOUNT + PROVIDER	NEW EMPLOYER ESTATE	BEHAVIOURAL LAYER
What left	Y: sync DB file list	Download + share events	Volume + destination service	Y: the received files	What arrived	References in messages
How it left	Y: client, browser, rules	Sharing, forwarding, sync	Y: the connection record	Upload method	Receipt artefacts	"I put it in my Drive"
When (choreography)	Y: sync timestamps	Y: event times	Y: connection times	Upload times	Access times	Resignation + joining dates
Where it went	Account in client config	Destination address in share	Y: destination host	Y: the account itself	The account it came from	Named in messages
Who did it	Profile context	Y: acting account + session	Source machine + user	Account holder	Recipient identity	Y: the person's own words

Fallback strategy in one line: read the endpoint and platform for what left and where, bound it from the network, reach the material at the destination through process: and when one stage was cleaned, the transfer's other four still recorded it.

Worked examples

EXAMPLE 1 · THE PERSONAL DRIVE THAT MIRRORED THE WHOLE DESK

A sales director resigned; within a week his replacement found clients already being courted by his new venture. The §4 examination of his sequestered laptop found a consumer Google Drive client signed into a personal Gmail address, its local database listing 6,400 corporate files mirrored over the final three weeks, with paths spanning the entire client and pricing folders; the browser held the account's session and the "add to Drive" activity; and the corporate M365 audit log (§5) showed the matching mass downloads. The §6 preservation letter and undertakings reached the personal account, imaged by an independent examiner: it held all 6,400 files, upload timestamps corroborating the sync database to the minute, and, tellingly, a further share of the pricing folder to his new co-founder's address. The §7 manifest and choreography grounded a springboard injunction and delivery-up; the second share extended it to the co-founder. The USB era's single copy had become a continuous, doubly-recorded mirror.

EXAMPLE 2 · THE FOLDER THAT WAS SHARED, NOT DOWNLOADED

An engineer left a firm with, apparently, nothing: no USB records, no personal sync client, a clean browser. The employer nearly closed the file. The §5 platform audit log told the real story: in his final fortnight he had shared the entire CAD library folder: 40 GB, thousands of drawings: to a personal email address by creating an internal-then-external share, and had shared a second folder by anonymous link, the link's usage log showing it followed three times from an IP range matching his home. No data had been "taken"; access had been granted to a destination he controlled from outside. The §6 process reached the personal account (which had by then downloaded the library) and the anonymous-link destination. The lesson is §3's: sharing is exfiltration, it leaves no download and no USB trace, and the platform audit log is the only near-end witness: which is why it is exported first.

EXAMPLE 3 · THE SYNC THAT WAS SANCTIONED, AND THE CLAIM THAT NARROWED

An employer alleged wholesale cloud theft against a departing consultant, citing a personal OneDrive client on her laptop with thousands of files. The §7 innocent-explanation pass, run by the respondent's examiner, reframed most of it: the personal OneDrive had been installed and sanctioned years earlier under the firm's explicit BYOD-and-home-working policy (produced in evidence), its sync database showed continuous mirroring of her own working folder throughout her tenure exactly as the policy permitted, and comparable consultants' laptops showed the identical pattern. But the same examination found what was not sanctioned: in her final week, a browser upload of the firm's central client database export: a file outside her working folder and outside the policy: to a personal Dropbox created that day. The claim narrowed to the one genuine transfer, which was proven precisely and returned; the wholesale allegation, which would have failed, was never run. The pass protected the respondent from the true claim's cost and the applicant from the false claim's collapse.

Common mistakes and technical limitations

Common mistakes

- **"It went to the cloud, so it's gone":** the transfer treated as unprovable when both ends and the network recorded it: §2's exactly-wrong assumption.
- **Sharing overlooked:** Example 2's folder: the audit log unexported while the investigation hunted for downloads and USBs.
- **The destination never pursued:** the near-end proven, the personal account left un-preserved and emptied: §6's letter sent too late or not at all.
- **Sync separated from choice imperfectly:** the sanctioned personal sync of Example 3 pleaded as theft, or the genuine upload lost among it.
- **Audit logs left to expire:** the platform's record of the transfer aged out during internal deliberation: guide 105 §6's clock.
- **Endpoints released:** the laptop with the sync database reissued before imaging: guide 97 §3's afternoon, for cloud.
- **Manifest by adjective:** "substantial data" pleaded where the sync database and destination account offered a file list.
- **Breach clocks missed:** client personal data known to have left, the employer's own UK GDPR notification never assessed.

Technical limitations

- **Network logging varies:** proxy, DLP and CASB coverage depends on deployment; a home-working transfer over a personal network may bypass corporate egress logging entirely: the endpoint and destination carry more weight, and the report says so.
- **Destination access needs process:** the personal account is reached through law, on legal timelines the strategy must price in: the near-end evidence stands alone until it is.
- **Provider cooperation is jurisdictional:** consumer cloud providers' disclosure processes and locations vary: planned early where the account holder will not cooperate.
- **Sync databases can be cleaned:** uninstalling the client removes some residue; the corporate sync record, credential store, platform log and destination survive (guide 110 §6).
- **Baselines decide meaning:** Example 3's lesson: without the policy and role baseline, sanctioned sync over-accuses; the examiner builds it first.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What personal cloud and BYOD use does your policy sanction, and where is it documented: the Example 3 baseline?
- Have the platform audit logs, DLP alerts and proxy logs been exported, and are the leavers' devices sequestered unhandled?
- Did any client personal data form part of what may have left, so the breach clocks are assessed now?

Ask your opponent (the former employee / new employer)

- Please identify all personal or third-party cloud storage and webmail accounts to which our client's data has been uploaded, synchronised, shared or forwarded, and preserve those accounts and their contents unaltered, providing the enclosed undertakings as to non-use, non-disclosure and delivery-up.
- Please provide a list of all our client's files or folders transferred to or shared with any such account, the dates and methods of transfer, and confirmation of any onward sharing, downloading or copying from those accounts, including to [the new employer].
- (To the new employer:) Please confirm what data originating from our client has been received into your systems or any personal account of [the employee], the steps taken to quarantine it, and your preservation of all relevant records.

Ask your eDiscovery / forensic provider

- What does the sync database list, and does the platform audit log corroborate it?
- What does the network layer say about volume and destination where the endpoint is silent?
- Has the destination account been preserved, and does the innocent-explanation pass leave the transfer standing?

SUGGESTED WORDING · CLOUD-EXFILTRATION PRESERVATION AND UNDERTAKINGS (FIRST LETTER)

"Our client's forensic examination evidences the transfer of its confidential data to personal or third-party cloud storage and/or webmail accounts under your control, including [category summary], in the period [dates]. You are required immediately to: (1) preserve, without deletion, alteration, downloading, sharing or use, all such accounts and their contents, including [identified accounts]; (2) provide within [7] days the enclosed undertakings as to non-use, non-disclosure, preservation and delivery-up; (3) identify all files and folders so transferred or shared, all accounts and devices to which they were synchronised, and all persons to whom any part has been disclosed or shared; and (4) permit forensic examination of the accounts and any synchronising device on terms to be agreed, by an independent examiner if preferred. In default, our client will apply without further notice for delivery-up, imaging and injunctive relief, including springboard relief, and will rely on this letter on costs. Where the accounts are held with a third-party provider, our client reserves the right to seek disclosure from that provider directly."

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

The cloud-exfiltration checklist

- ☐ Devices sequestered unhandled; sync databases and browser artefacts preserved
- ☐ Platform audit logs, DLP alerts and proxy/CASB logs exported same week
- ☐ Sharing and anonymous-link events searched, not just downloads
- ☐ Auto-forwarding rules and connected apps enumerated
- ☐ Destination accounts identified from endpoint configuration and platform shares
- ☐ Preservation letter and undertakings sent before accounts can be emptied
- ☐ Destination reached by undertaking, order or provider process
- ☐ File-level manifest built and reconciled across near and far ends
- ☐ Sensitivity classified; UK GDPR breach clocks assessed
- ☐ Innocent-explanation pass run against policy and role baselines

Red flags

- Consumer sync clients signed into personal accounts on work machines: Example 1's mirror.
- External or anonymous shares of whole folders in the leaving period: Example 2's link.
- Auto-forwarding rules to personal addresses.
- Mass downloads preceding personal-cloud connections in the proxy log.
- Uploads outside sanctioned folders or policy: Example 3's Dropbox.
- Personal accounts emptied after a preservation letter.
- Client personal data in the transferred set, unnotified.

When to involve a digital forensic expert

At the trigger, before the device is touched or the account can be emptied: containment and the §11 letter are same-day work; through the near-end examination, where the sync database, platform audit log and network layer are read together into a manifest; at the destination, where undertakings, orders and provider process reach the account and its material (Example 1's imaged Drive); at assessment, where the innocent-explanation pass separates sanctioned sync from genuine theft (Example 3); and at deployment, under CPR Part 35 at injunction speed, on either side. Through **cflab.uk** and **e-discovery.uk**, cloud-exfiltration investigations run from same-week preservation to injunction evidence: and the personal account, reached in time, holds both the proof and the property.

§ 13 · COMMON QUESTIONS

Frequently asked questions

The data went to a personal cloud account. Can we even prove it?

Yes, and usually well: the corporate machine's sync database or browser artefacts name the files and the account (§4), the platform audit log records the downloads or shares (§5), the network bounds the volume, and the destination account: reached through process: holds the material itself (§6). Example 1 was proven at both ends to the minute. The cloud feels elusive and is in fact doubly-recorded.

The employee just shared a folder rather than downloading anything. Is that exfiltration?

Squarely: sharing corporate content to a personal or external address, or creating a link and taking it away, moves the data to the employee's control without a download or a USB trace (§3, Example 2): and it is logged as a sharing event with the destination in the platform audit trail, which is why that log is exported first when downloads and USBs come up empty.

Can we get into the employee's personal cloud account?

Through process, not self-help: a preservation letter and undertakings first, then delivery-up and imaging orders, commonly via an independent examiner who reports only on your material and protects the employee's private data (§6, guide 97 §7): the account holds both the manifest and the files. Where the holder will not cooperate, the provider's records are reached by disclosure. Plan the route early; the account can be emptied in minutes.

The employee had a sanctioned personal cloud for home-working. Does that defeat the claim?

Only for what it sanctioned: the innocent-explanation pass (§7, Example 3) separates policy-permitted sync of the employee's working folder from unsanctioned transfers outside it, and the genuine exfiltration usually stands out clearly against the baseline. Running the pass first protects both sides: it narrows an over-broad claim to what will survive, and clears what was legitimate.

How fast do we need to move?

Same-day for preservation of the near-end evidence and the destination account: audit logs expire, the personal account can be emptied, and springboard relief dies of delay (guide 97 §7): Example 1's account still held everything because the letter reached it in the first week. The manifest can be built afterwards; the preservation cannot be redone.

Does the employer have its own obligations if client personal data left?

Yes: a transfer of client personal data to an uncontrolled personal account is a personal-data breach with UK GDPR notification questions on the ICO's clock (guide 99 §6): assessed from the manifest's sensitivity classification (§7) as the investigation proceeds, not after. The exfiltration investigation and the breach assessment run together.

§ 1 4 · REFERENCE

Glossary

Anonymous link

A share reachable by anyone with the URL, taken away for later use.

CASB

Cloud-access-security-broker logging of sanctioned and unsanctioned cloud use.

DLP

Data-loss-prevention tooling that flags and logs policy-matching transfers.

Destination account

The personal or third-party cloud account receiving the data.

Egress record

The network's log of outbound connections, volumes and destinations.

External share

Granting an outside address access to corporate content.

Manifest

The file-level schedule of exactly what was transferred.

Personal sync client

A consumer cloud client signed into a personal account on a work machine.

Staging

Gathering corporate files locally before upload.

Sync database

A cloud client's local record of every mirrored file.

Sources and authoritative references

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

- cflab.uk, digital forensics services (cloud-exfiltration investigation, sync and egress analysis, injunction-speed CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Identification and Phase 04 · Collection (endpoint, platform and destination collection as practised): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- CPR Part 25 (interim remedies, including delivery-up and injunctions): justice.gov.uk, [Part 25](#) · CPR Part 31 (r.31.17 third-party disclosure): justice.gov.uk, [Part 31](#) · CPR Part 35: justice.gov.uk, [Part 35](#)
- ICO, employment monitoring and personal data breach guidance: ico.org.uk, [report a breach](#) · UK GDPR resources: ico.org.uk
- PD 57AD: justice.gov.uk, [PD 57AD](#) · ISO/IEC 27037: iso.org, [27037](#)

DISCLAIMER

This publication provides general information about investigating data exfiltration to cloud storage as at August 2026. Platform logging, sync-client behaviour, network tooling and provider disclosure processes change; verify the current position for the systems and matter at hand, and take advice on personal-device and personal-account access. 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

Cloud-exfiltration work at **e-discovery.uk** runs the transfer's stages at injunction speed: same-day containment and the §11 preservation letter before the destination account can be emptied; near-end examination reading the sync database, browser artefacts and platform audit log into a file-level manifest, with the network layer bounding what the endpoint cannot show and the sharing events a download-hunt would miss (Example 2); the destination reached by undertaking, order or provider process and imaged by an independent examiner (Example 1's 6,400 files); the choreography timed and the innocent-explanation pass run against policy and role baselines before anything is sworn (Example 3); and the sensitivity classified so the employer's own breach clocks are assessed. Reports run under CPR Part 35 for springboard and confidential-information relief, on either side. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a resignation landed this week, the audit logs are ageing and the personal account is a click from empty: preservation is today's task.



I N S T R U C T T H E L A B

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