COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Remote Employee Collection

Preserving and Collecting Evidence From Devices You Cannot Put Your Hands On

The custodian works from home in another county, or another country. The laptop that holds the evidence is on their kitchen table, not in the building. The dispute requires that its contents be preserved and collected defensibly, but nobody from the firm or the laboratory can walk up to it, and often the custodian is the very person whose conduct is in issue. Remote collection is now the ordinary case, not the exception: distributed workforces, home working and bring-your-own-device have moved the evidence out of the server room and onto devices scattered across the map. The methods have matured to meet this: remote forensic agents, guided self-collection, cloud-side collection that never touches the device, and shipped write-blocked media. Each trades convenience against completeness and control, and each carries its own defensibility and data-protection questions. This guide sets out for UK lawyers how remote collection is done, when each method is appropriate, how to preserve a device you cannot touch, and how to keep a remote collection defensible when the custodian is cooperative, reluctant or adverse.

⏱ Estimated reading time: 24 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Remote collection is now routine laboratory work: agent-based and cloud-side collection, supervised self-collection, and shipped write-blocked imaging across distributed and international workforces: scoped for defensibility and data minimisation, documented for reproducibility, and reported under CPR Part 35 and CrimPR Part 19 where the manner of collection is itself in issue.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | REMOTE & AGENT COLLECTION | SUPERVISED SELF-COLLECTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: REMOTE COLLECTION IS THE ORDINARY CASE NOW, AND IT IS DEFENSIBLE WHEN THE METHOD IS MATCHED TO THE CUSTODIAN'S COOPERATION AND THE EVIDENCE REQUIRED: AGENT, CLOUD-SIDE, SUPERVISED SELF-COLLECTION OR SHIPPED MEDIA, EACH DOCUMENTED, VERIFIED AND DATA-MINIMISED, WITH THE DEVICE PRESERVED THE MOMENT THE DUTY ARISES

The methods (§3): remote forensic agents deployed over the network to image or targeted-collect a device under examiner control; cloud-side collection that gathers the custodian's mailbox, drives and SaaS records without touching the device at all (guides 111 to 114); supervised self-collection where the custodian operates under live remote guidance; and shipped write-blocked media or the device itself couriered to the laboratory. **Choosing (§4):** the method follows cooperation (adverse custodians never self-collect), the completeness required (a full image for deleted-data questions, targeted collection for known documents), the control needed (examiner-operated where the manner of collection may be challenged), and the risk (of spoliation, of overreach into private data). **Preserving the untouchable device (§5):** the hold notice that reaches the remote custodian, the cloud-side preservation that secures the synced copy immediately, and the instruction not to use, wipe or reset the device (guide 110) while collection is arranged. **Defensibility (§6):** chain of custody maintained across distance, hash verification proving the remote image is complete and unaltered, the collection logged and reproducible (guide 71), and the reluctant or adverse custodian handled by examiner-controlled methods and, where needed, court compulsion. **Data protection (§7):** the UK GDPR and privacy care that remote and personal-device collection demand: data minimisation, the personal-device boundary, and the independent-examiner model that collects the relevant material while protecting the custodian's private life (guide 97). **The whole (§8):** the estate's redundancy meaning the device is rarely the only source, and cloud-side collection often reaching the evidence without the device at all.

- **Remote is the norm:** distributed workforces put the evidence on devices nobody can walk up to: the methods have met it.
- **Method follows cooperation:** adverse custodians get examiner-controlled or cloud-side collection, never self-collection.
- **Cloud-side often skips the device:** the mailbox, drives and SaaS hold much of it, collected without touching the laptop.
- **Distance does not excuse defensibility:** hashes, chain of custody and reproducibility hold across the map.
- **Personal devices need the privacy model:** minimise, bound, and use the independent examiner to protect private life.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the evidence is on a device you cannot reach

Classical forensic collection assumes physical access: the device is seized, brought to the laboratory, and imaged on a bench with a write-blocker. The distributed workplace has quietly removed that assumption. The custodian whose laptop holds the case works from a spare room a hundred miles away, or from another jurisdiction entirely; the device is company-owned but never comes into the office, or is personally owned and never was the company's to seize. The old instinct, to get the device to the bench, still applies where it can, but in most modern matters it cannot happen quickly, cheaply or at all, and insisting on it wastes the days in which evidence is most at risk.

Remote collection answers this, and it is not a compromise so much as a different, mature discipline. Its central insight is that the device is often not the only place the evidence lives: the custodian's mailbox, cloud drives and SaaS records hold much of it and can be collected server-side without the device (guides 111 to 114). Where the device itself is needed, remote agents and supervised methods can image or collect it across the network with the same hash-verified defensibility as a bench image. The art is in matching the method to the custodian and the evidence, preserving the device you cannot touch while you arrange the collection, and keeping the whole exercise defensible and proportionate at a distance. This guide takes those in turn.

§ 0 3 · THE METHODS

The methods: agents, cloud-side, supervised self-collection and shipped media

- **Remote forensic agents:** a forensic agent deployed to the device over the network (through the organisation's device-management or a sent installer) that images the disk or performs targeted collection under the examiner's remote control: examiner-operated, hash-verified, and the closest remote analogue to a bench image: the method of choice for company-managed devices where completeness and control matter.
- **Cloud-side collection:** collection of the custodian's mailbox, cloud drives, file-sharing platforms and SaaS records directly from the provider, server-side, without touching the device at all (guides 111 to 114): often the fastest and least intrusive route, reaching much of the modern evidence estate while the device question is resolved separately.
- **Supervised self-collection:** the custodian operates their own device under live remote guidance from the examiner (screen-shared, step-by-step), running a provided collection tool or copying identified material to supplied media: appropriate only for cooperative custodians and lower-stakes material, with the supervision and its limits documented.
- **Shipped write-blocked media or device:** a write-blocker and collection kit couriered to the custodian for a supervised image, or the device itself couriered to the laboratory under a documented chain of custody: slower but yielding a full bench-grade image where the matter demands one and the device can be released.
- **Hybrid, sequenced approaches:** cloud-side collection first to secure the estate immediately, then an agent or shipped image of the device for completeness: the common real-world pattern, securing the perishable now and the complete later.

§ 0 4 · CHOOSING THE METHOD

Choosing the method: cooperation, completeness, control and risk

- **Cooperation first:** a cooperative custodian widens the options (supervised self-collection, shipped kit); a reluctant or adverse one narrows them to examiner-controlled agents, cloud-side collection the custodian cannot interfere with, and court compulsion: the custodian whose conduct is in issue never self-collects (guide 97's exit-investigation logic).
- **Completeness required:** deleted-data, timeline and anti-forensic questions (guides 106 to 110) need a full forensic image (agent or shipped); known-document and mailbox questions are met by targeted or cloud-side collection: the method matched to what must be recovered, not to habit.
- **Control and challenge:** where the manner of collection may itself be challenged (adverse party, criminal exposure), examiner-operated methods with full logs are chosen over anything the custodian touches: the collection able to withstand cross-examination on how it was done (guide 100).
- **Risk of spoliation:** where there is a real risk the custodian will destroy or alter data, cloud-side preservation is engaged first and immediately (it cannot be interfered with from the device), and the device secured by agent or order before the custodian can act (guide 110 §7).
- **Proportionality and cost:** shipping a device across a jurisdiction for a full image is justified where the matter needs it and disproportionate where cloud-side collection answers the question: the method sized to the dispute (guide 20's balance).

§ 0 5 · PRESERVING A DEVICE YOU CANNOT TOUCH

Preserving a device you cannot touch

- **The reaching hold notice:** a preservation notice served on the remote custodian that names the device and accounts, instructs against use, deletion, wiping, resetting and encryption (guide 110 §11), and explains that these acts are traceable and carry consequences: the preservation duty delivered to a person you cannot supervise.
- **Cloud-side preservation immediately:** holds placed on the mailbox, drives and SaaS records server-side the moment the duty arises (guides 105 §6, 114 §6): the synced and cloud copies secured at once, independent of the device and beyond the custodian's reach.
- **Suspend automated deletion:** device-management retention, backup rotation and platform lifecycle policies suspended for the custodian's data (guide 113 §6): the automation that would delete evidence halted while collection is arranged.
- **Secure the account, manage the device:** for an adverse custodian, disabling further sync or access to prevent exfiltration or destruction while preserving what exists, balanced against alerting them: a judgement made with the litigation strategy, not a reflex.
- **Document the preservation:** what was preserved, when, how and by whom, recorded contemporaneously: the preservation itself part of the defensible record, and the answer to any later spoliation allegation (guide 95 §6).

§ 0 6 · DEFENSIBILITY

Defensibility: chain of custody, verification and the reluctant custodian

- **Chain of custody across distance:** the record of who collected what, when, how and from where, maintained though nobody was in the room: the agent's logs, the shipped media's courier trail, the supervised session's recording: the continuity documented despite the distance (guide 2's continuity principle, remotely applied).
- **Hash verification:** the remote image or collection hashed and the hash verified, proving the data received is complete and unaltered in transit (guide 3's fingerprints): the technical guarantee that a collection done over a network is as sound as one done on a bench.
- **Reproducible, logged collection:** the tool, scope, queries and parameters recorded so the collection can be explained and, where possible, repeated (guide 71): the method transparent to the other side and the court.
- **The supervision record:** for supervised self-collection, the examiner's contemporaneous record of what was instructed, what the custodian did, and what limits applied: the honest account of a method that depends on the custodian's hands, with its weight stated accordingly.
- **The reluctant and adverse custodian:** where cooperation fails, examiner-controlled agents and cloud-side collection that need no cooperation, and, where those are resisted or the device withheld, applications to compel (delivery-up, imaging orders, unless orders): the collection achieved through the court where it cannot be achieved by agreement (guide 97 §7).

§ 0 7 · DATA PROTECTION AND PRIVACY

Data protection, privacy and personal devices

- **Data minimisation at collection:** the collection scoped to relevant material by date, custodian and type wherever the method allows (targeted agent collection, scoped cloud-side queries), rather than imaging everything, so minimisation begins at collection, not just review (guides 20, 97's data-protection frame).
- **The personal-device boundary:** a personally owned device is not the company's to image at will: collection proceeds by consent on defined terms, or by order, and reaches only the relevant material, with the custodian's private data protected: the bring-your-own-device problem handled as a legal question, not a technical one.
- **The independent-examiner model:** for personal devices and mixed-use company devices, an independent examiner images the device but discloses only the relevant material, filtering the custodian's private life from the collection (guide 97 §7): the model that reconciles the right to the evidence with the right to privacy.
- **Home-context data:** a home-working device and network may hold family members' data and domestic material: the collection and its scope designed to avoid sweeping in third parties' personal data (UK GDPR): the home context respected.
- **Transparency and lawful basis:** the employer's lawful basis for collecting from an employee's device, the applicable policies, and the transparency owed: addressed before collection, and recorded: the ICO's employment-monitoring expectations met (guide 99's data-protection discipline).

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a remote custodian's device is one node in a redundant estate, and remote collection reads the whole, not just the node it cannot reach. The device holds the local material and the deleted-data and anti-forensic record that only a full image yields. But the mailbox holds the correspondence server-side; the cloud drives and file platforms hold the documents (guides 111 to 112); the SaaS platforms hold the structured records (guide 114); the cloud infrastructure holds the account activity (guide 113); the device-management platform holds the device's compliance and location record; and the counterparties hold their side of every communication. When the device cannot be reached, cloud-side collection reaches most of the evidence without it; when the custodian is adverse and the device withheld, the server-side estate is collected regardless and the device compelled by order; when the device is personal and private, the independent examiner filters it and the cloud estate corroborates. The device matters most for what only it holds, deleted and local artefacts, and the estate carries the rest while that is arranged.

QUESTION	THE REMOTE DEVICE	MAILBOX + CLOUD DRIVES	SAAS + CLOUD INFRA	DEVICE-MANAGEMENT PLATFORM	COUNTERPARTIES	DELETED / LOCAL ONLY
Correspondence	Local cache	Y: server-side	Logged interactions	n/a	Y: their copy	Local drafts
Documents	Local copies	Y: synced + versioned	Attached to records	n/a	Shared copies	Local-only files
Structured records	n/a	Exported copies	Y: the platform	n/a	Their view	n/a
Device use + location	Y: local artefacts	n/a	Sign-in context	Y: compliance + check-in	n/a	Y: local timeline
Deleted / anti-forensic	Y: full image only	Version history	Audit trail	n/a	n/a	Y: unallocated, journals

Fallback strategy in one line: collect the server-side estate immediately and without the device; reach the device by agent, shipped image or order for what only it holds; and let cloud-side redundancy carry the case while the untouchable device is secured.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE COOPERATIVE CUSTODIAN AND THE SEQUENCED COLLECTION

A company needed to collect from a senior manager working permanently from home two hundred miles away, in an ordinary commercial dispute where his conduct was not in question. Speed and proportionality mattered more than a full image. The §3 sequenced approach fitted: cloud-side collection of his mailbox and OneDrive was completed the first day, server-side, reaching the bulk of the relevant correspondence and documents without touching his laptop; a remote forensic agent, deployed through the company's device management with his cooperation, then performed a targeted collection of the local project folders the cloud did not hold, hash-verified under the examiner's control. No device was shipped, no bench image was needed, and the §6 logs made the collection fully reproducible. The whole exercise took three days and a fraction of the cost of couriering the device to London, and the §7 minimisation, scoping the agent collection to the relevant folders, kept it proportionate. The ordinary remote case, handled the ordinary modern way.

EXAMPLE 2 · THE ADVERSE CUSTODIAN WHO WAS NEVER ALLOWED TO SELF-COLLECT

A departing employee suspected of taking confidential data was, extraordinarily, asked by the client's HR team to "copy anything relevant onto a memory stick and send it in". The laboratory stopped that at once: an adverse custodian self-collecting is an invitation to selective disclosure and destruction (guide 97, guide 110), and the memory-stick request would have destroyed the defensibility of everything. The §4 method was reset to examiner control: cloud-side preservation and collection of the mailbox, drives and CRM were run server-side and immediately, beyond the employee's reach (§5); and when the employee, now on notice, declined access to his company laptop, the §6 route was an imaging order, executed by an independent examiner. The server-side estate had already secured the manifest of what he had taken (guide 111); the ordered image of the device supplied the anti-forensic evidence of his attempts to clean it. The lesson is §4's first rule: the person whose conduct is in issue never touches the collection.

EXAMPLE 3 · THE PERSONAL DEVICE AND THE INDEPENDENT EXAMINER

An employment claim required collection from a claimant's personal phone, which she had used for work messaging: her own device, holding her private life alongside the relevant work chats. A demand to image the whole phone for the employer to review would have swept in her family photographs, health data and personal correspondence, and she resisted it rightly. The §7 independent-examiner model resolved it: an agreed independent examiner imaged the phone, applied search terms and a date range agreed through the tribunal directions, and disclosed only the relevant work-related messages, holding the rest under the examiner's control and never passing it to the employer. The §7 minimisation and the personal-device boundary were honoured; the relevant evidence was collected in full; and the claimant's private life was protected. The model reconciled the two rights that a whole-phone image would have set against each other, and both sides accepted the result.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Adverse custodians asked to self-collect:** Example 2's memory stick: the defensibility destroyed and destruction invited at a stroke.
- **The device insisted on when the cloud held the answer:** weeks and cost spent shipping a device for material the mailbox and drives already contained.
- **Preservation delayed by the collection debate:** the argument over method run while the data was unpreserved: cloud-side preservation is instant and should precede the debate (§5).
- **Whole personal devices imaged for review:** Example 3's avoided error: private life swept into disclosure without the independent-examiner filter.
- **Distance treated as excusing defensibility:** hashes, chain of custody and logs skipped because "it was remote": the collection unable to survive challenge.
- **Supervised self-collection over-relied on:** used for high-stakes or contested material it cannot bear, its custodian-dependence unstated.
- **Automated deletion left running:** device-management and backup retention deleting the custodian's data during the collection delay (§5).
- **Lawful basis unaddressed:** employee and personal-device collection run without the data-protection groundwork the ICO expects (§7).

Technical limitations

- **Agent collection needs connectivity and access:** a device offline, off the domain, or beyond device management cannot be reached by agent: the shipped or ordered route remains.
- **Cloud-side does not reach local-only data:** material never synced, and the deleted-data and anti-forensic record, live only on the device: the full image is still needed for those (§8).
- **Bandwidth bounds full remote imaging:** imaging a large disk over a home connection is slow; targeted collection or shipped media may be more practical: the constraint planned for.
- **Supervision is not control:** a supervised custodian's hands are still their hands; the method's weight is lower than examiner-operated collection, and honestly stated.
- **Jurisdiction shapes everything:** a device or custodian abroad engages the cross-border questions of guide 116: remote collection across a border is a legal exercise before a technical one.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Where are the relevant custodians and their devices, are the devices company-managed or personal, and how cooperative is each custodian likely to be?
- What cloud and SaaS estate can be preserved and collected server-side today, independent of the devices?
- What is the lawful basis and policy position for collecting from employees' and personal devices?

Ask your opponent (or a reluctant custodian)

- Please preserve, and not use, alter, wipe, reset or encrypt, the device(s) identified, and confirm the same in writing, pending arrangements for forensic collection by an agreed method.
- Please confirm whether the device(s) are company-managed or personally owned, their location, and your proposals for defensible collection, including whether you consent to examiner-operated remote collection or an independent-examiner imaging of any personal device on agreed terms.
- Please confirm that automated deletion, backup rotation and device-management retention affecting the relevant data have been suspended.

Ask your eDiscovery / forensic provider

- Given this custodian's cooperation, location and the evidence required, which method, and why?
- What can we preserve and collect cloud-side today, and what genuinely needs the device?
- How will the remote collection be verified and logged so it withstands challenge?

SUGGESTED WORDING · INSTRUCTION FOR A REMOTE COLLECTION

> "We instruct you to preserve and collect the electronic evidence of the custodian(s) identified at Schedule 1, who work remotely at the locations stated. Please: (1) place immediate server-side holds on their mailboxes, cloud drives, file-sharing and SaaS accounts, and confirm the same today; (2) advise on the appropriate collection method for each custodian and device, having regard to the custodian's cooperation, the completeness required, the need for examiner control, and proportionality, distinguishing what can be collected cloud-side from what requires the device; (3) for any device requiring collection, propose an examiner-operated remote agent, shipped write-blocked imaging, or supervised collection as appropriate, and for any personally owned device, an independent-examiner model scoped by agreed search terms and date ranges to protect private data; (4) maintain chain of custody and hash verification throughout and record the method, scope and parameters so the collection is reproducible; and (5) scope all collection to relevant material by date, custodian and type to observe data minimisation. Report any indication that a device has been used, wiped or reset since preservation was requested."

§ 12 · QUICK CONTROL

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

The remote-collection checklist

- ☐ Custodian locations, device ownership and cooperation assessed
- ☐ Server-side holds placed on mailbox, drives and SaaS the same day
- ☐ Automated deletion and backup rotation suspended
- ☐ Hold notice reaching the remote custodian; no-use instruction given
- ☐ Method matched to cooperation, completeness, control and risk
- ☐ Adverse custodians never self-collecting
- ☐ Chain of custody and hash verification maintained across distance
- ☐ Collection scoped for data minimisation by date, custodian, type
- ☐ Personal devices handled by consent or order and the independent-examiner model
- ☐ Method, scope and parameters logged and reproducible

Red flags

- An adverse custodian asked to gather their own evidence: Example 2.
- A whole personal device demanded for the other side to review: Example 3's avoided error.
- The collection-method debate running while data is unpreserved.
- Devices offline or off device management, unreachable by agent.
- Supervised self-collection proposed for contested, high-stakes material.
- Signs a remote device has been used or reset since preservation was asked for.
- Employee or personal-device collection with no lawful-basis groundwork.

When to involve a digital forensic expert

At the first sign the evidence sits on a device nobody can reach, because server-side preservation is same-day and the method choice shapes everything after it; at method selection, where cooperation, completeness, control and risk are weighed and the adverse-custodian rule applied (Example 2); at collection, where agent, cloud-side, supervised or shipped methods are run with chain of custody and hash verification intact across the distance (Example 1); on personal devices, where the independent-examiner model reconciles the evidence with privacy (Example 3); and at deployment, where the manner of a remote collection is explained and defended under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, remote collections run from same-day server-side preservation to verified, defensible delivery, for cooperative and adverse custodians alike: because the device may be out of reach, but the evidence does not have to be.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can a device be collected forensically without anyone touching it?

Often, yes: a remote forensic agent images or targets it over the network under the examiner's control, hash-verified like a bench image (§3); and much of the evidence is collected cloud-side from the mailbox, drives and SaaS without the device at all (guides 111 to 114). Where only the device holds something, deleted or local-only data, an agent, shipped image or order reaches it. Distance no longer means the evidence is unreachable.

Can we just ask the employee to send us the relevant files?

Only if they are cooperative and the material is low-stakes, and even then under supervision (§3): an adverse custodian, or anyone whose conduct is in issue, must never self-collect, because it invites selective disclosure and destruction (§4, Example 2). For those, examiner-controlled or cloud-side collection that needs no cooperation is used, and the court compels access if it is withheld.

The custodian works from home abroad. Does that change things?

Substantially: a device or custodian in another jurisdiction engages cross-border collection, data-transfer and sometimes blocking-statute questions before any technical step (guide 116). Cloud-side collection may still reach the estate through the UK-controlled provider account, but collecting from a device abroad is a legal exercise first: take the cross-border advice before acting.

How do we collect from a personal device without invading privacy?

Through the independent-examiner model (§7, Example 3): an agreed independent examiner images the device but applies agreed search terms and date ranges and discloses only the relevant material, holding the private remainder and never passing it to the other side. Combined with collection by consent or order and data minimisation, it reconciles the right to the evidence with the right to a private life.

Is a remote collection as defensible as a bench image?

When done properly, yes: the image or collection is hash-verified to prove it is complete and unaltered, the chain of custody is maintained though nobody was in the room, and the method and scope are logged and reproducible (§6). Examiner-operated remote methods carry the same weight as a bench image; supervised self-collection carries less, and its custodian-dependence is stated honestly.

What do we do the moment we know a remote custodian is relevant?

Preserve server-side immediately, before debating method: holds on the mailbox, drives and SaaS are instant, beyond the custodian's reach and independent of the device (§5); suspend automated deletion; and send the reaching hold notice instructing against use, wiping and reset. The method choice can follow; the preservation cannot wait, because the device you cannot see may be being used right now.

§ 14 · REFERENCE

Glossary

Remote agent
Forensic software collecting a device over the network under examiner control.

Cloud-side collection
Gathering data server-side from the provider, without the device.

Supervised self-collection
A custodian collecting under live remote guidance.

Shipped imaging
A write-blocker kit couriered for a supervised image.

Chain of custody
The documented history of who held and handled evidence.

Hash verification
Proving a collection is complete and unaltered by digital fingerprint.

Independent examiner
A neutral examiner filtering relevant from private data.

Data minimisation
Collecting only what is relevant, from the outset.

Device management
The platform administering company devices remotely.

BYOD
Bring-your-own-device; personally owned devices used for work.

Sources and authoritative references

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

- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (remote, agent, cloud-side and supervised collection as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- cflab.uk, digital forensics services (remote and independent-examiner collection, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- PD 57AD (disclosure duties and preservation): justice.gov.uk, PD 57AD · CPR Part 31 and PD 31B: justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- ICO, employment practices and monitoring at work guidance (lawful basis, personal devices, transparency): ico.org.uk, employment · UK GDPR resources: ico.org.uk
- ISO/IEC 27037 (identification, collection, acquisition and preservation of digital evidence): iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Remote collection at **e-discovery.uk** starts with the two things that cannot wait: same-day server-side preservation of the mailbox, drives and SaaS estate, and the reaching hold notice that instructs the remote custodian against use, wiping and reset. The method then follows the custodian and the evidence: cloud-side collection where it answers the question, an examiner-operated remote agent where the device holds more, shipped write-blocked imaging where a full bench-grade image is needed, and supervised self-collection only for cooperative custodians and lower-stakes material, with the adverse-custodian rule absolute (Example 2). Personal devices are handled through the independent-examiner model, scoped by agreed terms and dates to protect private life (Example 3). Every collection is hash-verified, chain-of-custody documented and logged for reproducibility, and scoped for data minimisation. Reports run under CPR Part 35 and CrimPR Part 19 where the manner of collection is in issue. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a relevant custodian is working from a kitchen table somewhere you cannot reach, preservation of their cloud estate is a task for 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