COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Identifying the Right Custodians in Electronic Disclosure

People, Shared Sources and Organisational Data

What a custodian actually is, how custodial and non-custodial sources differ, and how to handle the categories that break the simple model: shared mailboxes, departmental repositories, service accounts, former employees and organisational data. With a structured custodian interview question set and the tiering method that keeps custodian lists proportionate and defensible.

⏱ 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. Its eDiscovery arm, **e-discovery.uk**, opens every matter with identification: custodians, repositories and scope, logged as the first entry in the chain of custody, before forensic collection, processing, hosted review and production. That work makes custodian scoping a daily discipline for our team, from negotiating custodian lists in Disclosure Review Documents to extracting the personal devices of departing directors under consent protocols. Our examiners also produce CPR Part 35 and CrimPR Part 19 compliant expert reports where examination follows.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ISO 27001-ALIGNED SECURITY | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | PD 57AD / DRD EXPERIENCE | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE ANSWER: WHAT IS A CUSTODIAN?

A custodian is a person (or, by extension, an identity) whose data holdings are treated as a unit of collection, search and review in a disclosure exercise. "The finance director" as a custodian means her mailbox, her chat accounts, her drives, her devices and her share of the systems she uses, gathered, deduplicated and searched as one bundle attributable to her. The custodian is the organising unit of eDisclosure: custodian lists are what the Disclosure Review Document records, custodian counts are what drive cost, and custodian selection is where most scope arguments are actually won or lost.

- **Not everything has a custodian.** Shared mailboxes, departmental drives, CRM and ERP systems, service accounts and log data are non-custodial: they belong to a function or to the organisation, and they need a nominated system owner rather than a custodian. Treating them as custodial (or forgetting them because they have no name attached) is the most common structural error in disclosure planning.
- **Selection runs from issues to people, never the reverse.** The pleaded issues identify the events; the events identify the roles; the roles identify the people; interviews and cross-checks then test the list. Starting from the org chart produces seniority-based lists that miss the assistant who actually ran the project.
- **Tier, then negotiate.** Core, secondary and peripheral tiers let you propose a proportionate list with a principled basis for resisting expansion and a ready mechanism for staged extension. A flat list of names invites a flat demand for more.
- **Former employees stay on the list.** Leaving employment does not remove a person's data from the client's control, and PD 57AD expressly contemplates preservation notices to former employees. The questions are practical: what survives, where, and what cooperation is needed.
- **The interview is the instrument.** §12 provides a structured custodian interview set (role, communication habits, identities and aliases, delegation, storage behaviour and leaver context) whose signed record becomes part of the identification evidence behind the disclosure certificate.

§ 0 2 · FIRST PRINCIPLES

What is a custodian? The concept in plain English

The word comes from the idea of custody: the person who "keeps" a set of documents. In paper litigation it was literal (the files in someone's cabinet). In electronic disclosure it is a modelling choice: the industry organises sprawling data estates by attaching each source to the person whose working life generated it. One human, many sources, one unit of work:

ONE CUSTODIAN: "A. PATEL, COMMERCIAL DIRECTOR"	TYPICALLY BUNDLES
Identity	a.patel@client.com plus any aliases and prior addresses (apatel@, patel.a@, the pre-merger domain)
Mail	Mailbox, archives, PSTs, litigation-hold and recoverable-items stores
Chat	Teams or Slack account (DMs and private channels), WhatsApp and SMS on work and consented personal handsets
Files	OneDrive or Drive, home-drive folder, desktop and downloads on assigned devices
Devices	Laptop(s), phone(s), tablets, including replaced units still in storage
System footprint	Her user activity inside CRM, ERP and other business systems (notes, edits, exports, logins)

Why the concept earns its central place:

- **Procedure asks for it.** The Disclosure Review Document under PD 57AD, and the Electronic Documents Questionnaire under PD 31B, both require the parties to identify whose data will be searched. Custodian lists, with date ranges per custodian, are the currency of that exchange.
- **Cost scales by it.** Collection is priced per source, processing per gigabyte, review per document, and all three multiply with each added custodian. The difference between eight and sixteen custodians is usually the largest single cost decision in the case.
- **Technology is built around it.** Deduplication can run globally or per custodian, search reports break down by custodian, and review platforms present custodian as a first-class field. A clean custodian model makes every downstream stage cleaner.
- **Attribution flows from it.** "Found in the custodian's mailbox" is the beginning of most authorship and knowledge arguments. Where sources are shared, that inference weakens, which is exactly why the non-custodial categories in §§6 to 10 need their own handling.

> FOR THE PRACTITIONER
>
> Keep two vocabularies straight. A custodian is a unit of the disclosure exercise. A witness is a unit of the trial. The lists overlap heavily but are not the same: a custodian may never give evidence, and a witness may have generated no data. Conflating them produces custodian lists built for advocacy rather than for finding documents, and both exercises suffer.

§ 0 3 · THE DISTINCTION

Custodial and non-custodial sources: the distinction that organises everything

Every source in the data map should carry one of two labels, because the label determines who answers for it, how it is collected, and how its contents are attributed:

	CUSTODIAL SOURCES	NON-CUSTODIAL SOURCES
Definition	Data generated by and attributable to an identified person's working activity	Data belonging to a function, team, system or the organisation itself, with no single human owner
Examples	Personal mailboxes, individual chat accounts, OneDrive, assigned devices, personal phones used for work	Shared mailboxes, departmental drives and SharePoint sites, CRM and ERP, finance systems, service accounts, logs, CCTV, backups
Who answers for it	The custodian, via interview and questionnaire	A nominated **system owner** (the person who administers or best understands it), via the IT and systems questionnaire
Collection unit	Per custodian, per source	Per repository, site, database or report
Attribution strength	Strong: presence in the mailbox supports knowledge and authorship inferences	Weak by default: presence proves the organisation held it; authorship and knowledge need logs, metadata or testimony
Classic failure	Missing the personal device or the second email address	Missing the source entirely because no custodian claims it, or over-collecting a whole repository when a subtree would do

The practical rule: **every source gets exactly one accountable human**. For custodial sources that human is the custodian; for non-custodial sources it is a named system owner recorded in the data map. Sources with nobody accountable are the ones that get forgotten, and sources with two accountable people are the ones where each assumed the other dealt with it.

§ 0 4 · METHOD

Selecting custodians: from issues to people

Custodian selection is an evidence exercise, and it runs in one direction:

Figure 1 · Issues to people, not org chart to people. Each pleaded issue is decomposed into the events and decisions behind it; each event names roles (who negotiated, who approved, who executed, who recorded); roles resolve to individuals across the whole relevant period, including predecessors and leavers.

Practical techniques at step 4 and 5:

- **Chase the roles through time.** "The quality manager" may be three different people across the disclosure period. The role goes on the list; interviews resolve it to names and dates.
- **Look below the obvious seniority line.** Assistants who ran diaries and inboxes, project coordinators who kept the tracker, the analyst who built the model: junior custodians frequently hold the richest and most candid material.
- **Use the data to test the list.** Sample the first-collected mailboxes for correspondents: senders and recipients who appear heavily on the issues but are not on the list are candidate custodians (and the same analysis run on the opponent's Initial Disclosure tests their list).
- **Record every exclusion.** "Considered and excluded: M. Roy, copied on 40 emails, purely administrative role, no independent involvement" is one sentence in the data map and a complete answer eighteen months later.
- **Keep the list living.** Amendments to pleadings, review findings and analysis (communication maps especially) all generate custodian candidates mid-matter. A versioned list absorbs additions as routine; a static one makes each addition look like an admission.

§ 0 5 · THE DECISION

The tiering decision tree

Run each candidate through four questions and assign a tier. Tiers convert directly into DRD proposals: full collection and search for Tier 1, targeted collection for Tier 2, preserve-only for Tier 3, reasoned exclusion for the rest.

QUESTION 1

Was this person a direct participant in the events behind a pleaded issue (negotiated, decided, approved, performed, recorded)?

YES

Tier 1 (core). Full custodial collection across mail, chat, files and devices; full date range; include in every search.

NO

Continue to Q2.

QUESTION 2

Did they supervise, advise on or support those events closely enough to hold material the participants would not (board oversight, legal or finance input, the assistant who managed the correspondence)?

YES

Tier 2 (secondary). Targeted collection: defined sources, narrowed date ranges, issue-specific search terms. State the narrowing in the DRD.

NO

Continue to Q3.

QUESTION 3

Is there a realistic prospect they hold unique relevant material (a plausible side channel, a disputed meeting they attended, a candidate flagged by correspondent analysis)?

YES

Tier 3 (peripheral). Preserve now (hold notice, no reissue of devices), collect only if review or analysis later justifies it. Cheap insurance, honest DRD entry.

NO

Continue to Q4.

QUESTION 4

Merely copied, senior, or nearby?

EXCLUDE, WITH REASONS

Record the name, the consideration and the reason in the data map. Copy-line presence alone does not make a custodian; their material exists in the participants' collections already.

BUT RE-RUN ON CHANGE

New pleadings, new review findings and communication analysis re-open the question. Diarise it.

Figure 2 · Four questions per candidate. The tiers are also the negotiation: an opponent demanding fifteen custodians can be offered Tier 3 preservation for the marginal names, which protects the evidence while the argument about collection is had on proportionality grounds.

§ 0 6 · DIFFICULT CATEGORIES

Shared mailboxes

Every organisation runs them: info@, sales@, accounts@, complaints@, projects@. They are frequently where the operative correspondence with the counterparty actually happened, and they break the custodian model in three ways that need managing rather than lamenting:

- **They are non-custodial.** Collect them as repositories in their own right, with a named system owner, on the source list independently of any individual. The commonest failure is assuming a shared mailbox is "covered" because two of its users are custodians: their personal collections will not contain messages handled entirely inside the shared box by someone else.
- **Attribution needs extra evidence.** "Sent from accounts@" does not say who typed it. Establish the access list over time (who had rights, when), look for send-as versus send-on-behalf records, delegated-access logs and initials or names in signatures, and treat authorship of important shared-mailbox messages as a fact to be proved, not assumed. Where a message matters and authorship is disputed, that is log-and-artefact territory.
- **Scope can be tamed.** Shared mailboxes are often huge and mostly irrelevant. Date ranges, counterparty domain filters and issue-specific terms narrow them defensibly; say so in the DRD rather than silently sampling.

> **IDENTIFICATION QUESTIONS THAT FIND THEM**
>
> "Which shared or team mailboxes exist, and who has access to each?" · "Which of them were used to correspond with [counterparty] or about [the events]?" · "Do any auto-forward into personal mailboxes, or vice versa?" · "Who administers them, and is there an access-change history?"

§ 0 7 · DIFFICULT CATEGORIES

Departmental repositories

Shared drives, SharePoint sites, Teams channels' file tabs, project workspaces, the department's Dropbox: repositories owned by a function rather than a person. Handling principles:

- **List them as sources, not as appendages of custodians.** A project site used by nine people is one repository, collected once, not nine partial copies via nine custodians' sync folders.
- **Collect by subtree, not by drive.** The defensible unit is the project or matter folder tree relevant to the issues, identified with the system owner, collected with structure and permissions metadata intact. Whole-drive collection is the repository equivalent of imaging every laptop: occasionally justified, usually not.
- **Version history and access logs are part of the repository.** SharePoint version chains show how the contested specification evolved; access and sharing logs show who touched it and when. Ask for them at collection, because platform log windows expire (see the volatility guidance in our companion guide *Finding the Evidence*).
- **Permissions are evidence.** Who could see the folder is often as material as what was in it, particularly in confidential-information and knowledge disputes. Capture the permission state at collection and, where available, its change history.

§ 0 8 · DIFFICULT CATEGORIES

Service accounts and automated data

Service accounts are identities operated by software rather than people: scanner@ delivering scans to mail, noreply@ sending system notifications, integration accounts moving data between platforms, robotic process automation running overnight jobs. They matter more than their obscurity suggests:

- **They carry evidence.** The scanner account's sent items date-stamp when a paper document entered the digital estate. Notification accounts record approvals, sign-offs and workflow steps. Integration accounts' logs show data moving between systems, including data later said never to have existed.
- **They have no interviewee.** Assign each to the system owner of the platform it serves, and scope it through Part B of the systems questionnaire rather than expecting any custodian to mention it.
- **They confuse attribution if unmapped.** Messages "from" a service account can be triggered by a human action recorded elsewhere; conversely, a human account operated by automation (mailbox rules, delegated bots) can send without the human's involvement. Where authorship of an automated-looking message matters, map the trigger chain with the administrator before drawing inferences.
- **Watch for humans hiding in service identities.** Shared administrative logins ("admin", "warehouse1") used by rotating staff are service accounts in form and shared custodial sources in substance. Establish who used them, when, from the rota, shift records or logs.

§ 0 9 · DIFFICULT CATEGORIES

Former employees

Departure changes the practicalities, not the relevance. A leaver who was central to the events is a Tier 1 custodian whose data happens to be at risk. Work the category in four steps:

- **1 · Freeze the leaver pipeline.** On day one, instruct IT to suspend account deletion, mailbox purges and device reissue for all relevant leavers, and to report which relevant leavers are already in the pipeline. PD 57AD expressly contemplates written preservation notices to relevant former employees; send them.
- **2 · Inventory what survives.** Per leaver: mailbox (live, archived, or exported before deletion), OneDrive and home drive, chat accounts, devices in storage, and their footprint in shared and organisational systems (which survives them entirely). The gap between what existed at departure and what survives now is itself a fact to record.
- **3 · Assess control and cooperation.** Company-held data is squarely in the client's control. Data on the leaver's personal devices and accounts is a negotiation: contractual survival clauses, the preservation notice, and a cooperation request for interview and consented targeted extraction. Hostile leavers convert the question into one for the litigation itself (delivery-up, springboard relief, third-party disclosure), which is a reason to start politely and early.
- **4 · Interview if you can.** A leaver interview covers the same ground as §12 plus: what did you hand over, to whom; what did you take, delete or wipe; which personal accounts or devices held work material; and who inherited your role and files. Where departure was recent and contentious, pair the interview with forensic preservation of their returned devices before anyone else touches them.

> **FOR THE PRACTITIONER**
>
> The single most expensive week-one omission in this whole subject is the relevant leaver whose laptop was reissued and whose mailbox hit its deletion date while the team debated custodian lists. The leaver questions in Part B of the systems questionnaire (companion guide, *Finding the Evidence*) exist to surface exactly this; ask them before anything else.

§ 10 · DIFFICULT CATEGORIES

Organisational data: CRM, ERP and the systems with no custodian

The transactional systems (CRM, ERP, finance, HR, quality, ticketing) hold the organisation's structured memory. Nobody "keeps" them; everybody feeds them. Handling principles:

- **Model them as organisational sources with system owners**, scoped through the systems questionnaire: what the system records, what reports it can produce, what audit trails it keeps, and who understands it.
- **Extract answers, not archives.** The defensible unit is the agreed report: the transaction listing for the disputed orders, the change history for the contested records, the activity log for the relevant users and period. Raw database dumps are unreviewable and usually disproportionate.
- **The audit trail is the prize.** Field-level change histories (who edited the record, from what value, to what, when) are where backdating and after-the-fact tidying become visible. Ask expressly whether audit history is enabled, for which fields, and for how long; the answer is sometimes an uncomfortable "since last year", which is itself worth knowing early.
- **Custodian activity inside organisational systems bridges the two models.** A custodian's CRM notes, ERP entries and login history are simultaneously organisational data and part of that person's evidential footprint; scope the per-user extracts for Tier 1 custodians alongside the organisational reports.

§ 11 · EDGE CASES

Delegates, contractors, directors and group identities

CATEGORY	THE ISSUE	THE HANDLING
Assistants and delegates	They send from the principal's mailbox, manage the diary, and hold their own parallel record	Where the principal is Tier 1, assess the assistant independently (often Tier 2); map delegated-access rights so "sent by" versus "sent on behalf of" is understood before attribution arguments start
Contractors and agency staff	Worked on client systems, or on their own kit under their own domain, sometimes both	Their activity in client systems is the client's data; their own devices and mailboxes engage control analysis and the contractor agreement. List them as custodians where they were participants, and send preservation notices to their employers where relevant
Directors and NEDs	Light corporate footprint, heavy personal-channel use (personal email, WhatsApp), board portals	Do not let the thin mailbox mislead: interview for personal channels, include board-portal repositories as organisational sources, and handle personal devices under consented targeted extraction
Group and multi-entity identities	One human, several hats: employed by Entity A, emailing for Entity B, on Entity C's board	Map identities per entity; control and privilege can differ across the hats, and the custodian list should say which entity's exercise each identity belongs to
Departed-and-returned staff and role-sharers	Broken date ranges, two people alternating one role or one mailbox	Date-bound the custodianship per person; treat the shared identity as a shared mailbox with an access history

§ 12 · THE INSTRUMENT

The custodian interview: question set and method

The interview turns a name on a list into a mapped set of sources and a signed record. Method first: interview each custodian individually (people disclose side channels alone that they will not mention in groups); use a fixed question set so coverage is provable; take notes against the questions and have the custodian confirm the record; and repeat in shortened form when circumstances change. For a full written questionnaire covering systems and devices in depth, use Parts A to C in our companion guide *Finding the Evidence*; the set below is the interview version, tuned to custodian scoping.

ROLE AND INVOLVEMENT

- 1 · Describe your role during [period], and how it touched [the events]. What changed over the period?
- 2 · Who did you work with on these matters, inside and outside the organisation? Who actually did the day-to-day correspondence?
- 3 · Who held your role before and after you? Who covered your absences?

IDENTITIES AND CHANNELS

- 4 · Every email address you have used for work in the period, including old addresses, other entities' domains and personal accounts used even occasionally.
- 5 · Every messaging channel used for anything work-related: WhatsApp, SMS or iMessage, Signal, Telegram, Teams or Slack DMs, LinkedIn messages, others. For each: with whom, on which devices, and any auto-delete settings.
- 6 · Which shared mailboxes or team channels did you use or monitor? Did you send from any of them?
- 7 · Did anyone have delegated access to your mailbox or send on your behalf? Did you have such access to anyone else's?

STORAGE AND SYSTEMS

- 8 · Where did you actually keep your working documents: which drives, sites, folders, and any locations only you used?
- 9 · Which business systems did you use (CRM, ERP, finance, quality, project tools), and what did you record in them about these matters?
- 10 · Any personal cloud storage, personal devices or home equipment used for work in the period?
- 11 · Any spreadsheets, trackers or informal databases you maintained that others relied on?

DEVICES AND EVENTS

- 12 · Every computer, phone and tablet used for work in the period, including replaced, repaired, reset or lost devices, with approximate dates.
- 13 · Since [the dispute arose], have you deleted, exported, moved or tidied anything potentially relevant, or changed any retention or auto-delete setting? (Candour now is protective; discovery later is not.)
- 14 · Is there anywhere else at all that material about these matters might exist that we have not covered, however unlikely?

CLOSING THE RECORD

- 15 · Read-back and confirmation: the custodian reviews the noted answers, corrects, and signs or confirms by email; the record is filed with the data map and referenced in the DRD narrative.

§ 13 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Org-chart custodianship.** Lists built from seniority rather than participation: six directors, no project coordinator, and the operative correspondence missed.
- **The copy-line trap in both directions.** Adding everyone ever copied (cost explosion) or excluding someone because they were "only copied" when the copies were how they supervised (evidence gap). Participation, not presence, is the test.
- **Shared sources assumed covered.** The shared mailbox and the project drive left off the list because "the custodians will have it". They will not, reliably.
- **Leavers discovered late.** The predecessor in the role, gone eighteen months, whose mailbox export nobody can now locate.
- **Identities under-mapped.** One custodian, three historical addresses, and searches run against only the current one.
- **Exclusions unrecorded.** The name that was considered and reasonably excluded, indistinguishable two years later from the name that was never considered at all.
- **The witness list wearing a custodian costume.** Custodians chosen to match the intended trial narrative rather than the data, which opposing correspondent analysis will expose.

Technical limitations

- **Custodian fields are assigned, not innate.** The platform's custodian label records where data was collected from, which is not always who authored it; shared sources and delegated sending need attribution evidence beyond the field.
- **Per-custodian deduplication changes what reviewers see.** Global dedupe shows each document once (efficient, but hides who else held it); per-custodian dedupe preserves possession evidence at higher review cost. Choose deliberately per matter and record the choice.
- **Departed custodians' cloud traces expire.** Deleted-account retention, sharing links and audit logs run on provider clocks; a leaver identified in month six may already be partly unrecoverable, which is an argument for early breadth in preservation even where collection stays narrow.
- **Identity resolution is imperfect.** Aliases, marriage-name changes, domain migrations and contractor addresses defeat naive per-address searching; build an identity table per custodian and search against all of it.

§ 14 · INTERROGATORIES

Questions for the opponent and the provider

Ask your opponent (DRD / EDQ / correspondence)

- Provide your custodian list with role, relevance rationale and date range per custodian, and the names considered but excluded, with reasons.
- How were custodians identified: from the issues, from interviews, from correspondent analysis? Who conducted the exercise?
- Which shared mailboxes, departmental repositories and organisational systems are on your source list independently of custodians, and who is the system owner for each?
- Which relevant custodians are former employees, what survives for each, and what preservation steps were taken, when?
- For each custodian: which identities and addresses are included, and are personal channels and devices addressed expressly?
- What is your deduplication scope (global or per custodian), and will custodian fields in the production reflect all holders or first-collected only?

Ask an eDiscovery / forensic provider

- How do you support custodian scoping: interview frameworks, correspondent and communication analysis, identity-resolution tooling?
- Can you run correspondent analysis on early collections to test our list and the opponent's, and what does it cost?
- How are shared mailboxes and repositories collected and labelled so attribution questions stay answerable (access lists, send-as records, permission snapshots)?
- What is your approach to leavers: archived-mailbox recovery, storage-device imaging, consented personal-device extraction?
- How do tier changes mid-matter work operationally: adding a custodian, promoting Tier 3 to collection, and what does each step cost?

§ 15 · DRAFTING AIDS

Suggested wording for instructions

DRD NARRATIVE: CUSTODIAN PROPOSAL (CORE PARAGRAPHS)

> "The Defendant proposes the following custodians, identified by mapping the Issues for Disclosure to the events and roles involved and confirmed by structured custodian interviews: [Tier 1 names and roles], for whom full custodial collection (mail, chat, files and devices, including identified personal channels) will be undertaken for the period [ ]; and [Tier 2 names], for whom targeted collection limited to [sources / narrowed ranges] is proposed for the reasons stated. The following non-custodial sources will be collected independently, each with a nominated system owner: [shared mailboxes; repositories; organisational systems by report]. The following individuals were considered and are not proposed, for the reasons recorded: [names and one-line reasons]. Preservation steps (including notices to the former employees listed) were taken on [date]. The Defendant will keep the list under review and will propose additions promptly if review or analysis identifies further custodians."

FORMER EMPLOYEE: PRESERVATION AND COOPERATION LETTER (CORE PARAGRAPHS)

> "We act for [client], your former employer, in a dispute concerning [one line]. Documents and communications from your period of employment may be relevant, including material on personal devices or accounts used for work. Please preserve, and do not delete, alter or dispose of, any such material, including messages in personal messaging applications, until further notice; automatic deletion settings affecting such material should be disabled. We would be grateful for your cooperation in a short interview about the systems and channels you used, and, where appropriate, a targeted, consented extraction of relevant material from personal devices, conducted by an independent forensic laboratory under a protocol that protects your personal information. Please confirm receipt and preservation within [7] days. [Where applicable: your attention is drawn to clause [ ] of your employment contract regarding company documents and cooperation.]"

SYSTEM OWNER NOMINATION (INTERNAL INSTRUCTION)

> "For each non-custodial source listed in Schedule 1 (shared mailboxes, repositories, business systems), the named system owner is responsible for: answering the systems questionnaire for that source; ensuring preservation steps for it are implemented and maintained; supporting scoped collection (including access lists, permission states and audit histories where available); and notifying the legal team before any change affecting the source. Ownership changes must be reported and reassigned in writing."

§ 16 · QUICK CONTROL

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

The custodian checklist

- ☐ Issues decomposed to events and roles; roles resolved to named people across the whole period
- ☐ Every candidate run through the tiering tree; tiers recorded with reasons; exclusions recorded with reasons
- ☐ Custodian interviews completed on the fixed question set; signed or confirmed records filed
- ☐ Identity table built per custodian (all addresses, aliases, domains, prior names)
- ☐ Shared mailboxes and departmental repositories listed as independent sources with system owners
- ☐ Service accounts mapped to system owners; shared logins resolved to their human users
- ☐ Relevant leavers identified; pipeline frozen; preservation notices sent; surviving data inventoried
- ☐ Organisational systems scoped by reports and audit trails, with per-user extracts planned for Tier 1 custodians
- ☐ Deduplication scope chosen and recorded; custodian-field semantics understood for production
- ☐ Correspondent analysis run on early collections to test the list; re-run diarised
- ☐ DRD narrative drafted from the above, including the living-list commitment

Red flags

- An opponent's custodian list that is a board list: all seniority, no doers, no assistants, no leavers.
- No shared mailboxes or repositories anywhere on a source list for a business that plainly runs on them.
- A key role's predecessor missing from every list and every interview.
- Heavy correspondents on the issues (visible in Initial Disclosure) absent from the opposing list, unexplained.
- A custodian interview that surfaces a personal channel followed by reluctance to address it in the DRD.
- "That mailbox was deleted under our normal policy" for a leaver who left after the dispute arose.
- Your own client proposing custodians by who will "look right" rather than who holds the documents.

When to involve a digital forensic expert

Bring in an examiner when custodian questions become artefact questions: authorship of shared-mailbox or service-account messages needs log and header analysis; a leaver's conduct around departure needs device examination before reissue; a custodian's answers at question 13 disclose deletion or resets; identity questions (who really operated an account) need attribution work; or personal-device material must be extracted once, defensibly, under a consent protocol. The companion guides *eDisclosure or Digital Forensics?* and *Finding the Evidence* cover the escalation triggers and the wider source map in full.

§ 17 · COMMON QUESTIONS

Frequently asked questions

What is a custodian?

The person (or identity) whose data holdings are treated as one unit of collection, search and review: their mailboxes, chat accounts, drives, devices and system activity, gathered and searched as a bundle attributable to them. The custodian is eDisclosure's organising unit: DRDs list custodians, costs scale by custodian count, platforms index by custodian, and attribution arguments usually begin from whose collection a document sat in. Sources with no single human owner (shared mailboxes, repositories, business systems, service accounts) are non-custodial and are handled as sources in their own right with a nominated system owner.

How many custodians is normal?

There is no normal, but there are patterns: modest commercial disputes commonly run 4 to 8, substantial B&PC claims 8 to 20, and regulatory or fraud matters more. The defensible number is the one the issues-to-people method produces, tiered so that collection effort matches involvement. A useful discipline: for every custodian beyond the first eight, be able to say in one sentence what unique material they plausibly hold.

Is a shared mailbox a custodian?

No. It is a non-custodial source: collect it as a repository with a system owner, establish its access history for attribution, and never assume it is covered by the individual custodians who used it. The same applies to departmental drives and business systems.

Do former employees count as custodians?

Yes, whenever they were participants: departure changes what survives and how you reach it, not whether they matter. Freeze the leaver pipeline immediately, send preservation notices (PD 57AD contemplates exactly this), inventory what survives, and negotiate cooperation for anything on personal devices or accounts.

Is the CEO automatically a custodian?

No. Seniority is not participation. A CEO who approved one board paper may be a Tier 2 or Tier 3 entry, or a reasoned exclusion, while their assistant is Tier 1. Equally, do not use non-participation as a shield where the interview or correspondent analysis shows the CEO ran the relationship over WhatsApp; the data, not the org chart, decides.

Can we add or remove custodians after the DRD?

Yes, and well-run matters usually do. Additions arising from review findings, amended pleadings or communication analysis are routine when the list was framed as living and the change is proposed promptly with reasons. Removals are rarer (preservation usually continues even where collection is dropped) and should be agreed or ordered, not silent.

§ 18 · REFERENCE

Glossary

Attribution
Linking a document or action to the person responsible for it; strong for custodial sources, evidential work for shared ones.

Correspondent analysis
Analysis of senders and recipients in collected data to test custodian lists and surface missed participants.

Custodial source
A source generated by and attributable to an identified person's working activity.

Custodian
The person or identity whose data holdings form one unit of collection, search and review.

Delegated access
Rights allowing one user to read or send from another's mailbox; the key to send-as versus send-on-behalf attribution.

Identity table
The per-custodian list of all addresses, aliases and domains searched as that custodian.

Leaver pipeline
The IT process that deletes accounts and reissues devices after departure; the first thing frozen on day one.

Non-custodial source
A source belonging to a function, system or the organisation, handled via a system owner rather than a custodian.

Per-custodian deduplication
Dedupe scope that keeps one copy per custodian, preserving possession evidence at higher review cost.

Service account
An identity operated by software (scanners, notifications, integrations); evidential but interview-less.

System owner
The named human accountable for a non-custodial source: its questionnaire answers, preservation and scoped collection.

Tiering
Grading custodians (core, secondary, peripheral) so collection effort, and the DRD proposal, match involvement.

Sources and authoritative references

Custodian-scoping practice in this guide draws on the EDRM phase notes and practice materials published by our e-discovery practice, referenced here as sources:

- e-discovery.uk, EDRM Phase 01 · Identification (custodians, repositories, scope, logged as the chain of custody's first entry): e-discovery.uk/edrm/identification
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection: e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, case notes including custodian-count and personal-device collection matters (38-custodian cross-border regulatory disclosure; solicitor-supervised personal-device protocol; departing-employee endpoint preservation): e-discovery.uk/expertise
- e-discovery.uk, Knowledge Centre practice notes on mobile and messaging evidence: e-discovery.uk/knowledge
- Practice Direction 57AD (preservation duties including former-employee notices; the Disclosure Review Document): justice.gov.uk, PD 57AD
- CPR Part 31 (including 31.8 control) and PD 31B with the Electronic Documents Questionnaire: justice.gov.uk, Part 31 · PD 31B
- Attorney General's Guidelines on Disclosure (rev. 2024, digital materials): gov.uk, AG's Guidelines
- ICO, UK GDPR guidance including employment practices and monitoring: ico.org.uk
- Data Protection Act 2018: legislation.gov.uk/ukpga/2018/12 · Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/21

- EDRM, Identification stage standards: edrm.net, stages standards

DISCLAIMER

This publication provides general information about custodian identification in electronic disclosure in the United Kingdom as at August 2026. It 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. Rules, guidance and legislation change; always check the current text. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Custodian work is where our e-discovery practice (**e-discovery.uk**) and our forensic laboratory meet daily: structured custodian interviews and identity resolution; correspondent and communication analysis that tests custodian lists against the data; collection per tier, from full custodial capture of mail, chat, files and devices to targeted, consented extraction from directors' and leavers' personal handsets under solicitor-supervised protocols; shared-mailbox and repository collection with the access lists and permission states that keep attribution answerable; and, when authorship or conduct is disputed, laboratory examination reported under CPR Part 35 / CrimPR Part 19. We advise candidly on tiering and will tell you when a proposed custodian adds cost without adding documents. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.

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