CFL ELECTRONIC EVIDENCE SERIES · GUIDE 5

Identifying the Right Custodians in Electronic Disclosure

Custodians, non-custodial sources, shared mailboxes, service accounts and former employees: a practical guide to building, prioritising and defending the custodian list — with a full custodian interview question bank.

For solicitors, barristers, litigation partners and associates, paralegals, in-house counsel, disclosure lawyers, investigators and litigation-support professionals in England & Wales.

COMPUTER FORENSICS LAB

cflab.uk · e-discovery.uk · ICO ZB395023 · NPCC · ISO 17025 aligned practice

Contents

1 Executive summary

Almost every decision in electronic disclosure flows from one deceptively simple question: **whose data are we going to search?** The people (and systems) selected are the custodians. Choose too few, or the wrong ones, and relevant — possibly adverse — documents are never found, searches must be re-run, credibility is lost and the court may intervene. Choose too many and processing, hosting and review costs multiply, deadlines slip and proportionality objections follow. The custodian list is therefore not an administrative appendix to the Disclosure Review Document ("DRD"): it is one of the most consequential strategic documents in the case.

This guide explains what custodians are, how they differ from non-custodial sources such as shared mailboxes, departmental repositories, service accounts and organisational systems of record, and how to build a defensible list from the pleadings and the issues rather than from the org chart alone. It sets out a step-by-step workflow, a tiering and prioritisation method that keeps custodian counts proportionate, and detailed treatment of the categories that cause the most trouble in practice: former employees, personal assistants and delegates, senior executives, personal devices and accounts (including the Court of Appeal's approach in *Phones 4U v EE*), contractors, and group companies.

The centrepiece is a structured custodian interview: how to run it, who should attend, how to document it, and a question bank organised by theme. It complements the broader custodian and source questionnaire in Guide 4 of this series (*Finding the Evidence*): Guide 4 maps the whole data landscape; this guide goes deeper on selecting, prioritising and defending the human custodians and the non-custodial sources that sit alongside them.

KEY MESSAGES

- **Issues first, people second.** Derive custodians from the issues for disclosure, not from seniority. The person who negotiated the clause matters more than the director who signed it.
- **Custodians are not the whole answer.** Shared mailboxes, departmental drives, service accounts and structured systems hold evidence that belongs to no single person. A custodian-only search misses them.
- **Interview early, document everything.** A short, structured interview with each candidate custodian is the cheapest insurance available against re-collection, missed sources and adverse costs.
- **Tier, sample, expand.** Start with a defensible core, test the marginal custodians with sampling and early data assessment, and record why each person was included or excluded.
- **Former employees and personal accounts need immediate attention.** Their data is the most likely to be deleted by routine IT processes, and the legal basis for reaching it is the most delicate.

2 Custodians in plain English

A **custodian** is a person who holds, or is responsible for, documents that may be relevant to a dispute. In practice the word is shorthand for a bundle of data sources associated with that person: their mailbox, their OneDrive or Google Drive, their Teams or Slack messages, their laptop and phone, their paper files, and any personal accounts or devices used for work. When lawyers and eDisclosure providers talk about "collecting a custodian", they mean collecting some or all of those sources for that person.

The term comes from the practical reality of modern organisations: documents are not filed centrally by subject; they accumulate around people. Two colleagues on the same project hold different fragments of the story — one has the WhatsApp thread with the supplier, the other has the draft spreadsheet that never went anywhere. Identifying custodians is the process of working out which people's fragments the case needs.

Not everything belongs to a person. A finance system records journals posted by dozens of users; a shared "sales@" mailbox is read by a whole team; a departmental SharePoint site is edited by anyone with access. These are **non-custodial sources** (sometimes "organisational data" or "systems of record"), and they must be identified separately, because no custodian interview will surface them reliably and no custodian-based collection will capture them.

THE CORE PROBLEM

The custodian list is usually settled early, under time pressure, on incomplete information — yet everything downstream depends on it: the preservation notices, the collection plan, the DRD, the search-term negotiations, the review budget and, ultimately, what the court and the opponent see. Errors are expensive in both directions. The discipline described in this guide exists to make the list **deliberate, documented and revisable** rather than assumed.

Two questions run through this guide. First, *who* should be on the list — which requires understanding the dispute, the organisation and the informal ways work is actually done. Secondly, *what counts as that person's data* — which requires understanding delegation, shared resources, device practices and the difference between the account and the human being. A departed employee's mailbox may survive the employee; a personal assistant may send half of a director's email; a "custodian" may turn out to be a service account operated by a script. The label is convenient; the underlying map of people and sources is what matters.

3 Why custodian selection matters legally

3.1 PD57AD and the Disclosure Review Document

In the Business and Property Courts, Practice Direction 57AD puts custodians at the centre of Extended Disclosure. Section 2 of the Disclosure Review Document requires each party to describe where documents are held, and specifically to identify the custodians (including former employees) whose data will be searched, together with date ranges and data sources per custodian. Where Models C or D are sought, search proposals are typically framed as combinations of *custodian + date range + source + search terms* — so an unexamined custodian is, in effect, an unsearched part of the disclosure exercise.

Three features of PD57AD make custodian thinking unavoidable:

- **The duty of cooperation (paras 2.3, 3.2 and 10.6).** Parties and their legal representatives must cooperate and engage constructively on the contents of the DRD, including custodians. A party that cannot explain who its custodians are, or why others were excluded, is not in a position to cooperate meaningfully — and judges notice.
- **Known Adverse Documents (paras 2.6-2.8 and 3.1(2)).** A company "knows" of adverse documents through persons with accountability or responsibility for the events in issue, or for the conduct of the proceedings — including those who have left (para 2.9 requires reasonable steps to check with relevant former employees). Identifying those persons is custodian identification under another name, and it applies under every disclosure model, even Model A.
- **Preservation (para 4).** The duty to preserve extends to documents held by employees, former employees, agents and third parties, and para 4.2(2) expressly requires written notification to relevant employees and former employees. You cannot send hold notices to people you have not identified.

3.2 CPR Part 31 cases

Outside the Business and Property Courts, standard disclosure under CPR Part 31 requires a "reasonable search" (r.31.7), and Practice Direction 31B requires the parties to discuss the categories of electronic documents, the custodians ("the individuals whose documents are to be searched"), date ranges and keyword searches before the first case management conference. The Electronic Documents Questionnaire (PD31B Schedule) asks directly about custodians, their devices and their accounts. The disclosure statement must describe the extent of the search; a statement silent or vague about custodians invites applications under r.31.12 for specific disclosure.

3.3 What goes wrong

- **Re-collection and re-review.** A custodian added late means new preservation risks, a second collection exercise, incremental processing and another review pass — often at a point in the timetable where costs cannot be recovered and extensions are needed.
- **Specific disclosure applications and adverse inferences.** Gaps in the custodian list are among the most common grounds for applications under PD57AD para 17 (failure adequately to comply) and para 18 (variation), and unexplained gaps in the communications of an obvious custodian invite submissions that evidence has been withheld or destroyed.
- **Costs sanctions.** Disproportionate custodian counts cut both ways: a party that insists on collecting 60 custodians when 12 would do may not recover the difference; a party that quietly searched 3 when 12 were plainly relevant may face indemnity costs on the application that follows.
- **Personal devices and accounts.** In *Phones 4U Ltd v EE Ltd* [2021] EWCA Civ 116 the Court of Appeal upheld orders requiring corporate parties to *request* that named custodians make personal devices and email accounts available for search (through an independent process), while stressing the voluntary nature of the request and the custodians' privacy rights. The case is now the reference point for reaching work communications on personal sources — and it presupposes that you know who the relevant custodians are.

PRACTICE POINT

Record the custodian decision trail contemporaneously: who was considered, who was included, who was excluded and why, and what each interview revealed. Under PD57AD para 20 the court may order a party to explain the steps taken; a dated decision log converts an awkward witness statement into an exhibit that writes itself.

4 Key terminology

Term	What it means in practice
Custodian	A person whose associated data sources (mailbox, files, chat, devices, cloud storage) are identified for preservation and possible search. In the DRD, custodians are listed with date ranges and sources.
Non-custodial source	A repository not attributable to one person: shared mailboxes, departmental file shares or SharePoint sites, databases, accounting/CRM/ERP systems, intranets, archives, backups, CCTV.
Data custodian (IT sense)	In IT governance, the administrator responsible for a system (e.g. the Exchange admin). Not the same as a disclosure custodian — but often the person who can tell you what exists and export it.
Custodian interview	A structured conversation with a custodian (or candidate) to establish their role, communications habits, devices, accounts, filing practices and knowledge of other sources. Documented and repeatable.
Data map / source map	The working document linking issues → people → systems → locations, with preservation and collection status per source. See Guide 4 for the full method.
Tiering	Ranking custodians (e.g. Tier 1 core, Tier 2 probable, Tier 3 contingent) so that collection and review effort follows likely evidential value.
Shared mailbox	A mailbox accessed by several users (e.g. sales@, invoices@). Messages sent "from" it may be attributable to any member; sent-item behaviour varies with configuration.
Delegate access	Rights allowing one user (often a PA) to read and send from another's mailbox or manage their calendar. "Send on behalf" and "send as" leave different metadata traces.
Service account	A non-human account used by systems or scripts (e.g. scanner@, workflow bots, integration accounts). Can send, receive and store documents no human custodian will remember.
Leaver / departed custodian	A former employee whose account may be deactivated, converted to a shared mailbox, exported or deleted under leaver processes — frequently on a 30/60/90-day timer.
Joiners-movers-leavers (JML)	The HR/IT lifecycle governing account creation, permission changes and deletion. Understanding the client's JML process tells you how fast leaver data disappears.
BYOD	Bring Your Own Device: personal phones/laptops used for work, usually under a mobile device management (MDM) policy. Raises control, privacy and collection questions (see §8.5).
Custodian de-duplication	Processing option removing duplicates within (or across) custodians. Cross-custodian de-duplication saves review cost but can obscure who held a document — see §14.
Organisational knowledge holder	A person interviewed not because their own data matters but because they know where things are: IT managers, records managers, PAs, long-serving administrators.

5 Custodial and non-custodial sources

A defensible disclosure exercise identifies both halves of the data landscape. The custodian list captures documents that accumulate around people; the non-custodial list captures documents that belong to functions, teams or systems. The DRD asks about both, and PD31B's questionnaire does too. The categories below are the ones most often missed.

5.1 Shared and functional mailboxes

Almost every organisation runs shared mailboxes: sales@, accounts@, complaints@, legal@, tenders@. They matter for three reasons. First, they often hold the *authoritative* record of a category of communication (every complaint, every invoice query) that individual custodians hold only patchily. Secondly, attribution is ambiguous: a message sent from a shared mailbox may have been written by any of its members, and depending on configuration the sent item may sit in the shared mailbox, the individual's mailbox, or both. Thirdly, they are easy to overlook because no custodian thinks of the shared mailbox as "theirs". Ask every interviewee which shared mailboxes they can access and which they actually use.

5.2 Departmental repositories

File shares ("the S: drive"), SharePoint sites, Teams channel files, Confluence spaces and departmental Google Shared Drives hold the working documents of teams: contract drafts, board packs, project folders, tender libraries. Access logs and version history may show who did what, but the content itself is non-custodial: collecting the ten custodians' OneDrives will not capture the project SharePoint site unless it is separately identified. Map repositories by department and by matter, not by person — the custodian interview questions in §10 are designed to surface them.

5.3 Service accounts, bots and integrations

Scanners that email PDFs to themselves, workflow systems that send approvals from noreply@, CRM integrations that log correspondence, finance robots that post journals: service accounts generate and hold documents with no human custodian. In investigations they matter twice over — first as sources (the scanner mailbox may contain the only copy of a signed document), and secondly because messages "from" a service account can conceal the human who triggered them. An IT interview, not a custodian interview, is how these are found.

5.4 Systems of record and structured data

Accounting systems, CRM, ERP, HR systems, document management systems, case management systems and bespoke databases are organisational sources in which "documents" are really records and audit trails. They rarely map to custodians at all (though user activity within them can attribute actions to people). Treat them as their own workstream: later guides in this series address databases, accounting systems, CRM and ERP in detail.

5.5 Archives, journals and backups

Email journaling archives (e.g. legacy Enterprise Vault, Mimecast, Proofpoint), retention archives in Microsoft Purview or Google Vault, and backup systems may hold custodian data that outlives the live account — including for leavers whose mailboxes were deleted years ago. When a candidate custodian's live data is gone, the archive and backup layer is the first alternative path (see Guide 4, §Backups, and §8.1 below).

> **RULE OF THUMB**
>
> For every issue in the case, ask two questions: **"whose job was this?"** (which yields custodians) and **"what system was this done in?"** (which yields non-custodial sources). A list built from only one question is half a list.

6 Building the custodian list: a practical workflow

The workflow below assumes a commercial dispute of moderate size; scale it up or down. Its output is a **custodian and source register**: one row per candidate custodian (or non-custodial source), with role, relevance to issues, date range, sources held, preservation status, tier, and an include/exclude decision with reasons.

1. **Start from the issues, not the org chart.** Extract the factual issues from the pleadings (or, pre-action, from the letter of claim and response). For each issue write down the events, decisions, documents and time periods it implicates. This is the same issues-to-sources translation described in Guide 4, §4 — reuse it.
2. **Identify the obvious actors.** The signatories, the negotiators, the complainers and the complained-about: people named in the pleadings, the contract, the correspondence already in hand. These are Tier 1 candidates almost by definition.
3. **Get the organisational context.** Obtain org charts for the relevant period (not just today's), project team lists, board and committee memberships, distribution lists for key emails, and the client's matter or project codes. Ask HR for joiners, movers and leavers across the relevant period — the org chart of March 2023 may bear little resemblance to today's.
4. **Mine the documents you already have.** The disclosure given pre-action, the key contract emails, the exhibits: who is on the To/Cc lines? Who is mentioned but never appears as a sender? Early data assessment on a seed collection (see Guide 8 topics) can rank communicants by volume and flag names the lawyers have not heard of.
5. **Interview the organisational knowledge holders.** Before interviewing custodians, interview the people who know the landscape: the IT manager (systems, JML process, retention, archives), the relevant department head (who actually did the work), and often a PA or team administrator (how documents really flowed). This ordering means custodian interviews start from an informed map.
6. **Interview candidate custodians.** Use the structured interview in §10. Every interview ends with the same two questions: *who else was involved?* and *where else would this material exist?* Expect the list to grow by a third and then stabilise — snowball sampling converges quickly in most organisations.
7. **Tier and decide.** Apply the tiering method in §7. Record inclusion and exclusion decisions with one-line reasons in the register.
8. **Preserve immediately, collect deliberately.** Preservation (hold notices, suspension of deletion policies, leaver-process freezes) should cover Tiers 1-2 and arguable Tier 3 custodians *as soon as they are identified* — preservation is cheap and reversible; collection and review are neither. Collection then proceeds tier by tier.
9. **Feed the DRD and keep the register live.** Section 2 of the DRD is populated from the register. Revisit the register at every major case event: statements of case amendments, disclosure of the opponent's custodian list, witness statements, and any EDA results that change the picture.

DELIVERABLE

If you keep only one artefact from this guide, keep the **custodian and source register**. It answers the DRD, drives the hold-notice list, briefs the provider, records proportionality decisions, and becomes the exhibit if the methodology is ever challenged. A spreadsheet is fine; keeping it current is what matters.

7 Tiering, prioritisation and proportionate custodian counts

Custodian counts drive cost more directly than almost any other variable: each custodian added typically brings a mailbox, a OneDrive, chat history and often a device — several gigabytes of data whose processing, hosting and (above all) review must be paid for. PD57AD para 6.4's proportionality factors (the nature and complexity of the issues, the importance of the case, the likely probative value of the documents, the number of documents, the ease and expense of retrieval) apply squarely to the question "how many custodians, and which?".

7.1 A three-tier model

Tier	Who	Treatment
Tier 1 — Core	Directly involved in the events in issue: negotiators, decision-makers, authors of key documents, the individuals whose conduct is complained of.	Preserve and collect all relevant sources early; full date range; searched under the agreed terms; named in the DRD.
Tier 2 — Probable	Supervisors, successors, team members on key threads, PAs of Tier 1 custodians, finance/HR/ compliance actors for specific issues.	Preserve now; collect now or on a short trigger; consider narrower date ranges or source subsets (e.g. mailbox only); sample before full review.
Tier 3 — Contingent	Peripheral names: copied occasionally, involved in one meeting, mentioned once. Plus "insurance" custodians whose relevance depends on how the case develops.	Preserve (hold notice and suspension of deletion) but do not collect. Record the trigger that would promote them. Review the tier at each case milestone.

The tier boundaries are argument, not arithmetic — but the structure forces the right conversations: preservation is broad and cheap; collection is narrower; review is narrowest. Most disputes with 40 hold-notice recipients resolve to 8-15 collected custodians and fewer actually reviewed in full.

7.2 Techniques that keep counts honest

- **Early data assessment.** Process Tier 1 first and examine communication patterns: who do the core custodians actually correspond with about the issues? Names with negligible relevant traffic are candidates for demotion; unexpected heavy correspondents are candidates for promotion — on evidence, not instinct.
- **Sampling marginal custodians.** Run the agreed search terms across a marginal custodian's mailbox and review a sample of the hits. A 2% responsiveness rate, mostly duplicates of Tier 1 documents, is a documented reason to exclude; a pocket of unique relevant material is a documented reason to include. Either way the decision is defensible.
- **De-duplication analysis.** If a candidate's data is 95% duplicative of already-collected custodians (typical for people on the same threads), full review adds little. Note the caveats in §14 about losing "who held it".
- **Date-range and source narrowing.** A custodian relevant to one issue for four months does not need a six-year, all-sources collection. Per-custodian ranges and source subsets are expressly contemplated by the DRD.
- **Phasing and agreement.** Where the parties disagree about marginal custodians, propose phasing: search the agreed core now, revisit the disputed names after review, with a mechanism (and preserved data) for adding them. Courts respond well to structures that defer cost until justified.

> **PRACTICE POINT**
>
> Never let exclusion mean non-preservation. The cases that go wrong are those where a Tier 3 name was excluded from *collection* and nobody suspended the leaver process or retention policy, so when the name became central a year later the data was gone. Preservation tracks the candidate list; collection tracks the tiers.

8 Special categories of custodian

8.1 Former employees

Leavers are the highest-risk category on any custodian list, for three reasons. First, **their data is on a timer**: most organisations delete or anonymise leaver accounts under JML processes 30-90 days after departure, and Microsoft 365 permanently purges a deleted unlicensed mailbox after a further short window unless a retention hold applies. Secondly, **they cannot be interviewed on demand**: cooperation depends on goodwill, severance terms, or contractual obligations that may or may not exist. Thirdly, **the duties still reach them**: PD57AD para 4.2(2) requires written notification to relevant former employees as part of preservation, and para 2.9 requires reasonable steps to check whether relevant former staff hold known adverse documents.

Practical sequence for each relevant leaver: (1) ask IT immediately whether the account still exists, in what state (active, shared-mailbox conversion, litigation hold, exported PST, deleted), and freeze any deletion; (2) check archives, journals and backups for the period before deletion; (3) check the leaver's line manager and team for the leaver's key documents (much of it survives in others' mailboxes and shared repositories); (4) consider whether the leaver personally retains work data (personal accounts, home devices, exported contacts) and what basis exists to request it; (5) record everything, because "what happened to X's mailbox" is a question you will be asked.

8.2 Personal assistants and delegates

Senior custodians often barely touch their own mailboxes. PAs read, file, delete and send; calendars are managed wholly by delegates; "the director's documents" may live in the PA's folder structure. Where a Tier 1 custodian has (or had) an assistant, treat the assistant as a presumptive Tier 2 custodian, and establish in interview: who had delegate rights and when; whether messages were sent "as" or "on behalf of" the principal; and where the principal's documents were actually filed. Delegation also complicates attribution — a message from the principal's account may have been written by the assistant — which matters when documents are put to witnesses.

8.3 Senior executives and board members

Executives raise volume and sensitivity together: long tenures, huge mailboxes, heavily privileged and commercially sensitive content, and a strong incentive for opponents to demand them precisely because they are burdensome. Resist both extremes. Including the CEO "because it looks thorough" can add hundreds of thousands of documents of marginal value; excluding an executive who personally made the disputed decision is indefensible. Use the issues: if the decision, knowledge or state of mind of a named executive is in issue, they are Tier 1 however inconvenient. Consider narrowed date ranges and targeted sources, and plan the privilege workflow early (§15). Board-level material (packs, minutes, resolutions) is usually better collected from the company-secretarial system or board portal than from individual directors — a non-custodial route to custodial-looking content.

8.4 Contractors, agency staff and outsourced functions

Contractors may work on client systems (in which case their accounts are custodial sources within the client's control) or on their own (in which case the documents may be held by a third party and control must be analysed — see Guide 6 in this series). Outsourced functions — payroll, IT support, customer service — mean that documents about the client's business sit with the provider, reachable via contract terms, cooperation or third-party disclosure applications (CPR r.31.17). Identify the arrangement in the IT and HR interviews, and do not assume that a person with a company email address is an employee.

8.5 Personal devices and personal accounts (BYOD)

Where custodians used personal phones, WhatsApp, Signal, SMS or personal email for work, relevant documents exist on sources the company does not directly control. The Court of Appeal in *Phones 4U v EE* [2021] EWCA Civ 116 confirmed that a court may order a party to *request* its custodians (and even former employees) to make personal devices and accounts available to an independent examiner for search, while emphasising that the request is voluntary, that custodians

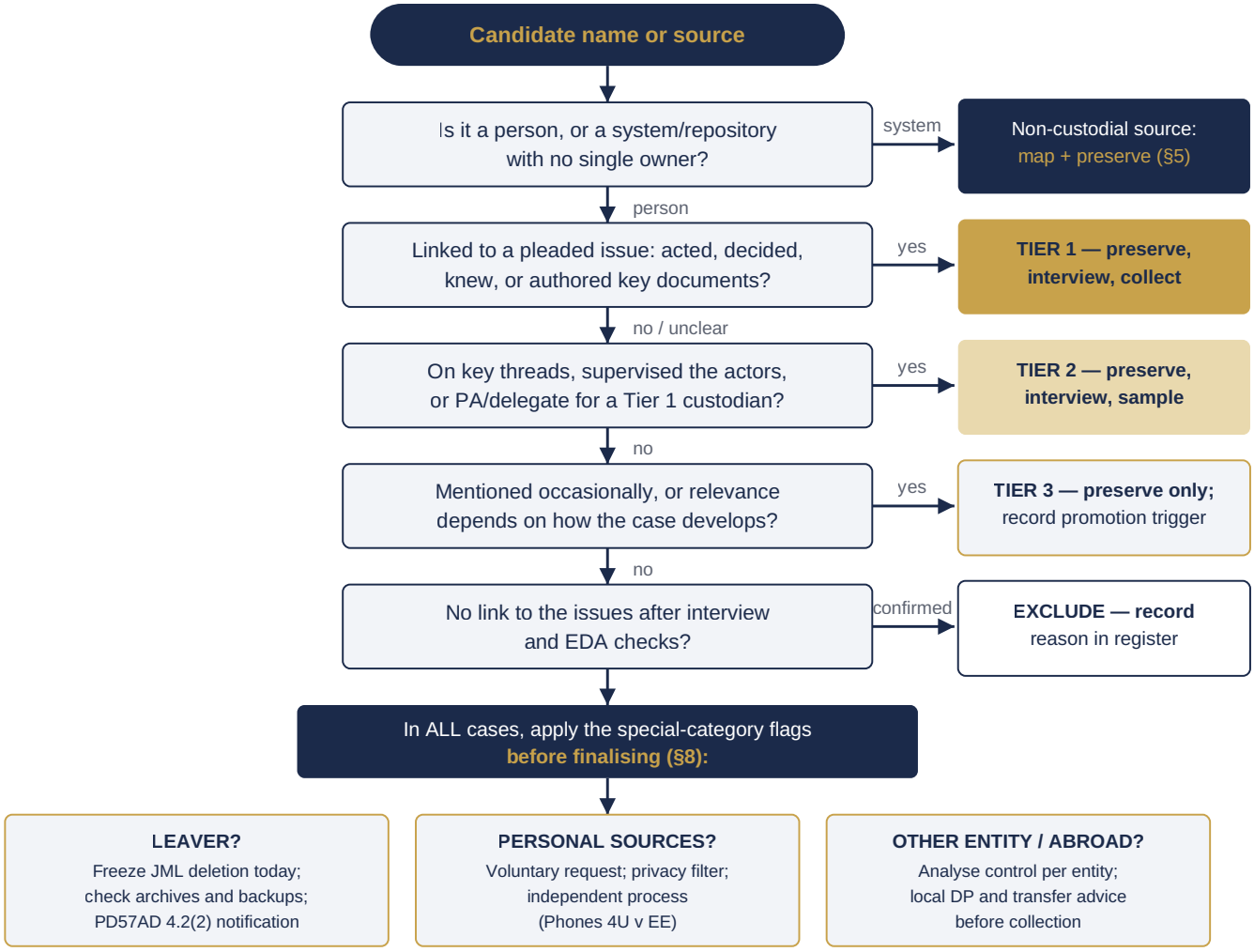
must not be misled about that, and that privacy (Article 8, UK GDPR) must be respected — typically via an independent forensic process that filters personal material before lawyers see anything. Practically: establish in every custodian interview whether work was done on personal sources (the interview questions in §10 cover this); if yes, preserve first by polite written request (stop deleting; do not reset the phone), and design a proportionate, privacy-respecting collection — a targeted extraction of identified chats, not a full phone image, is usually the right opening position. Guides 61-70 of this series cover mobile and messaging sources in depth.

8.6 Group companies and overseas custodians

Custodians employed by subsidiaries, parents or affiliates raise control questions (a party discloses documents in its control, which may or may not include other group members' documents) and data-transfer questions (overseas custodians bring local data protection, blocking statutes and employment law into play). Flag them early in the register, analyse control per entity, and take local advice before collecting from jurisdictions with strict transfer regimes. Guide 6 (control) and Guide 40 (multi-jurisdictional collection) address this in detail.

9 Decision tree: should this person or source be a custodian?

The tree below is a triage aid for each candidate name surfaced by the workflow in §6. It assumes preservation is cheap and collection is not — hence every exit on the right preserves before it decides.



Every exit preserves before it decides; only the tiers change what is collected and reviewed.

Figure 1 — Custodian triage: from candidate name to tiered, documented decision.

10 The custodian interview and question bank

The custodian interview is the single most cost-effective step in the whole exercise. Thirty to sixty structured minutes per custodian routinely surfaces the personal WhatsApp group, the departed colleague, the shared drive nobody mentioned and the "archive" folder on a home NAS — any one of which, discovered late, costs far more than every interview combined.

10.1 How to run it

- **Timing.** After the organisational-knowledge interviews (§6, step 5), as soon as practicable after the hold notice — while memories are fresh and before habits change.
- **Who attends.** A lawyer who knows the issues, plus (for technical custodians or complex environments) someone from litigation support or the forensic provider. Keep it small; it is an information-gathering conversation, not an examination.
- **Tone and framing.** Explain the purpose (finding where documents live, not judging conduct), the hold obligations, and that "I also used my personal phone" is a helpful answer, not a confession. Custodians who fear blame under-report sources.
- **Privilege.** Conduct the interview under legal professional privilege where it properly applies (a lawyer conducting it for the dominant purpose of litigation), mark the notes accordingly, and be aware that the *facts* learned (e.g. that a source exists) will still need to be acted on and may need to be disclosed in the DRD's description of sources.
- **Documentation.** A standard template per interview (the question bank below is designed as one), signed or email-confirmed by the custodian, filed against the register. Follow up in writing on any preservation actions the custodian must take.
- **Close the loop.** End every interview with the snowball questions (who else? where else?) and diarise a short re-check before the DRD is certified.

10.2 Question bank

Forty questions in seven groups. Groups A-F are for the custodian; Group G is for IT about the custodian. Guide 4's Parts A-C questionnaire covers the organisation-wide landscape; this bank is per-person and goes deeper on habits, delegation and personal sources. Adapt, cut and translate into plain language as needed.

A · Role and involvement

1. What was your role and title during the relevant period, and how did it change? Who did you report to, and who reported to you?
2. Describe your involvement in [the events in issue]: what did you do, decide, approve, draft or witness?
3. Which meetings, committees or approval chains touching the issues were you part of? Were they minuted, recorded or transcribed?
4. Who else was involved in these events, inside or outside the organisation? Who would know what you don't?
5. Did anyone involved leave the organisation? Who, when, and who took over their work and their files?

B · Communications habits

1. Which email accounts did you use for work (corporate, secondary, personal)? Did you ever forward work email to a personal account, and why?
2. Which chat and messaging tools did you use with colleagues and with external parties: Teams, Slack, WhatsApp, Signal, Telegram, SMS, iMessage, LinkedIn messages? For each: work account or personal, and with whom?
3. Are you in any group chats relating to the issues? Who administers them, and do they use disappearing-message settings?
4. Did you make or receive calls about the issues on platforms that record or transcribe (Teams, Zoom)? Do you use voicemail-to-email or dictation apps?
5. How do you handle attachments: send links (SharePoint/OneDrive/Drive) or copies? Where do links point?

C · Documents and filing

1. Where do you save your working documents: local drive, desktop, OneDrive/Drive, network shares, SharePoint/Teams sites, DMS? Show me your actual folder structure if possible.
2. Which shared or departmental locations did your team use for this work? Who set them up and who controls access?
3. Do you keep notebooks, diaries, task apps (OneNote, Notion, Evernote, paper)? Where are they?
4. Do you ever export, download or print reports from business systems (finance, CRM, ERP)? Which systems, and where do the exports go?
5. Have you deleted, archived or "tidied" any material relating to the issues — or run any cleanup tools — since the dispute arose? (Asked neutrally: the answer drives preservation, not blame.)

D · Devices

1. Which devices do you currently use for work: laptop(s), desktop, phone(s), tablet? Company-issued or personal? Managed by IT (MDM) or not?
2. What happened to your previous devices — upgrades, replacements, repairs? Were old devices returned, wiped, reissued or kept in a drawer?
3. Do you use USB sticks, external drives, memory cards or a home NAS for work material? Where are they now?
4. Do you sync work data to home computers or family-shared devices (shared iPad, family PC)?
5. Is anything encrypted or protected by passwords/PINs only you hold? Are you willing to provide access if needed?

E · Cloud and personal accounts

1. Which cloud storage do you use: OneDrive, Google Drive, Dropbox, iCloud, Box — work and personal? Any work files in the personal ones?
2. Do your phone backups go to iCloud or Google? Do you know when the last backup ran?
3. Do you use personal subscriptions for work tasks (personal Zoom, Canva, ChatGPT or other AI tools, file-transfer services like WeTransfer)?
4. Which social media accounts have you used to communicate about work matters relevant to the issues?
5. Would you be willing, in principle, to allow an independent forensic examiner to collect identified work material from personal devices or accounts, with personal content filtered out before the legal team sees anything? (Record the answer; do not press — see §8.5.)

F · Delegation and access

1. Does anyone have delegate access to your mailbox or calendar? Who sends emails as you or on your behalf?
2. Do you have delegate access to anyone else's mailbox? Whose, and how is it used?
3. Which shared mailboxes can you access, and which do you actually use? Do replies from them end up in your sent items or the shared account's?
4. Has anyone else ever used your accounts or devices (cover during leave, shared logins, "hot" desks or pool devices)?
5. Since the hold notice: do you understand what you must keep, and is anything automatic working against you (auto-archive, auto-delete rules, disappearing messages, phone storage optimisation)?

G · For IT, about this custodian

1. Account status: active, disabled, converted, deleted? On litigation hold? Since when?
2. Mailbox size, archive status, and any journaling or third-party archive coverage for this user and period?
3. OneDrive/Drive size and sharing report; Teams/Slack scope (channels, DMs) and applicable retention policies?
4. Devices issued to this user over the relevant period, per the asset register; current location and wipe/reissue history?
5. MDM enrolment for personal devices; what the MDM can and cannot see or wipe?
6. VPN, badge and system access logs available for this user and period, and their retention?
7. Any deletion, export or unusual admin activity on this account since the dispute arose (per audit logs)?
8. For leavers: exact JML steps already executed and the date the next irreversible step is due.
9. Any legacy systems this user's cohort used before migrations (old mail platform, previous DMS), and where that data went?
10. Who, other than central IT, administers any of this user's systems (departmental admins, external MSP)?

CROSS-REFERENCE

Guide 4 (*Finding the Evidence*), Part A-C questionnaire: organisation-wide systems, retention and third parties. Use Guide 4 once per client; use this bank once per custodian.

11 Worked examples: Aldgate Components v Harlow Precision

The recurring case study in this series: Aldgate Components Ltd terminated a long-term supply agreement with Harlow Precision Engineering Ltd, alleging repudiatory breach; Harlow counterclaims for wrongful termination and misuse of its confidential pricing information, and Aldgate separately alleges that a former Harlow employee took CAD files to a competitor. Three custodian problems from that dispute:

EXAMPLE 1 · THE SIGNATORY IS NOT THE NEGOTIATOR

Aldgate's first custodian list contained its CEO (who signed the 2019 agreement) and its current head of procurement. Interviews revealed that the agreement was negotiated by a procurement manager who moved to a group subsidiary in 2022, that her PA managed the negotiation correspondence through a shared "supplier-contracts@" mailbox, and that the price-review meetings in issue were minuted by a category analyst nobody had mentioned. The revised list: procurement manager (Tier 1 — located via HR, account on hold, still employed by the group), the analyst (Tier 1), the PA (Tier 2), the shared mailbox (non-custodial source), and the CEO demoted to Tier 3 with a narrowed date range covering the termination decision only. Cost of the interviews: under a day. Cost of discovering the analyst after the DRD was certified: an application, a supplemental collection and a wasted-costs argument.

EXAMPLE 2 · THE LEAVER ON A 60-DAY TIMER

Harlow's counterclaim named an Aldgate commercial director who had resigned four months before proceedings. Aldgate's JML process deletes leaver mailboxes 60 days after exit; the mailbox had been converted to a shared mailbox for handover, then scheduled for deletion in 12 days when the litigation team asked IT the right question. The mailbox was placed on hold the same day. His company phone, however, had been factory-reset and reissued — so his WhatsApp negotiations with Harlow's sales director were reconstructed from the counterpart device (Harlow's disclosure) and from his iCloud backup, which he voluntarily made available through an independent examiner after a *Phones 4U*-style request. The register recorded each step and date, which later answered Harlow's "spoliation" correspondence in two paragraphs.

EXAMPLE 3 · SAMPLING THE MARGINAL CUSTODIANS

Harlow proposed 31 Aldgate custodians for Model D searches. Aldgate's EDA on its eight Tier 1 custodians showed that 19 of the proposed names each appeared in under 0.5% of issue-relevant threads, almost entirely as Cc recipients of documents already captured. Aldgate ran the agreed terms across three of the 19 as a sample: responsiveness 1.8%, unique (non-duplicate) relevant documents: two. The parties agreed a final list of 13 custodians plus four non-custodial sources, with the remaining names preserved and a promotion mechanism recorded in the DRD. The sampling memo — one page — did more than six rounds of correspondence.

12 Custodians in the DRD and negotiating with opponents

12.1 Completing Section 2 of the DRD

Section 2 of the DRD asks each party to describe, per Issue for Disclosure where appropriate: the custodians whose documents will be searched (including relevant former employees), the date ranges applied to each, and the data sources per custodian. Practical drafting points:

- **Name roles as well as names.** "J. Patel (Commercial Director, 2019-2023; departed)" tells the opponent and the court why the person is there. Where names are sensitive, roles with initials can be discussed with the opponent — but the court will expect openness between the parties.
- **Per-custodian ranges and sources are your proportionality lever.** A blanket 2018-2026, all-sources statement wastes the structure the DRD offers. Narrow honestly and say why.
- **Include the non-custodial sources.** List shared mailboxes, repositories and systems alongside the human custodians so that the search description is complete — and so the opponent cannot later claim surprise.
- **Say what is not reasonably available.** If a leaver's mailbox was deleted pre-dispute under routine policy, the DRD (and any narrative) should say so, with dates. Volunteering the gap with its innocent explanation is far stronger than having it extracted.
- **Keep the certificate honest.** The DRD is signed with a statement of truth-equivalent obligations on the parties and legal representatives (PD57AD paras 3.2-3.3, 10.7). Certify only what the register supports.

12.2 Negotiating custodian lists

- **Exchange reasoning, not just names.** "We propose these 11 because..." invites agreement; a bare list invites suspicion. Ask the opponent for the same: their custodians' roles, date ranges and sources, and their reasons for exclusions you find surprising.
- **Watch the asymmetries.** An opponent proposing 40 of your custodians and 5 of theirs is making a costs argument for you. Equally, resist mirroring for its own sake — the right number follows the issues, and the issues may genuinely be lopsided.
- **Use the tools PD57AD gives you.** Disclosure Guidance under para 11 is a lightweight route to resolve custodian disagreements without a full application; phasing and sampling proposals (§7.2) give the court something to order other than a binary.
- **Ask about their leavers and personal sources.** If the opponent's key actor has left, ask in correspondence: what happened to the account, the devices, the chat data — and when. Early questions freeze positions before "routine deletion" can happen post-dispute.

13 Preservation and legal hold considerations

PD57AD para 4 requires parties to take reasonable steps to preserve relevant documents once proceedings are commenced or contemplated: suspending relevant deletion or destruction processes, sending written notification to relevant employees *and former employees*, and taking reasonable steps so that agents or third parties who may hold relevant documents do not delete them. The custodian register is the natural engine for all three. Custodian-specific points (Guides 21-30 of this series cover preservation in depth):

- **Hold notices track the candidate list, not the collection list.** Everyone in Tiers 1-3 (and arguable candidates) receives a hold notice with an acknowledgement; the register records send and acknowledgement dates and chase-ups.
- **Per-custodian IT actions.** For each custodian: litigation hold on the mailbox and OneDrive/Drive; suspension of Teams/Slack retention deletion for their scope; freeze on their JML steps if a leaver; asset-register check and quarantine of their devices before any reissue or repair; suspension of MDM wipe eligibility where feasible.
- **Personal sources are preserved by request, not seizure.** A written request to the custodian to retain identified personal-source material (stop deleting chats; do not reset or replace the phone without telling us) — polite, specific, documented. Legal compulsion, if ever needed, comes later and through the court.
- **Third-party custodians.** Agents, consultants and outsourced providers get preservation letters citing the client's contractual rights where they exist. Guide 29 covers drafting.
- **Re-verify before certifying.** Holds fail silently: licences lapse, policies change, an admin "tidies up". Before the DRD is certified and before production, re-confirm with IT that each hold is still in place — in writing.

14 Collection, metadata and attribution considerations

Custodian decisions shape the collection and processing stages in ways worth understanding before the DRD locks positions in:

- **Collect per custodian, per source, with documentation.** Each collection should record custodian, source, method, date, operator, scope and hash verification, so that any document in the review platform can be traced to a person, a source and a defensible acquisition. Guides 31-40 cover methodology; the point here is that the register's rows become the collection log's rows.
- **Custodian metadata is case metadata.** Processing platforms tag every document with its custodian(s). That field drives review batching, disclosure-list content and, later, cross-examination ("this was in your mailbox"). Errors made at collection (wrong custodian label on a PST; two people's data merged) are painful to unpick — check labels at handover.
- **Cross-custodian de-duplication: choose deliberately.** Removing duplicates across custodians can cut review substantially, but unless the platform records *all* custodians who held each document (an "all custodians" or "duplicate custodians" field), you lose the ability to say who held it — which can matter enormously ("the CFO had the memo" is the case). Insist on de-duplication that preserves the full custodian history, and confirm how the production will present it.
- **Attribution is not identity.** A document in a custodian's mailbox proves presence, not authorship or knowledge: delegates send as principals, shared logins exist, service accounts forward, and mailbox rules move messages unread. Where authorship or knowledge is contested, metadata and system logs (and sometimes forensic examination) do the attribution work — see §18 and Guide 87 (metadata).
- **Chat data is custodian-shaped but thread-centred.** Teams, Slack and WhatsApp collections are made per custodian but reviewed per conversation; the same thread collected from two custodians may differ (deletions, edits, join dates). Preserve both sides where possible — the counterpart copy is the classic alternative evidence path.

15 Privilege and confidentiality

- **Privilege-heavy custodians need a plan, not avoidance.** In-house counsel, company secretaries and executives who corresponded extensively with lawyers will generate large privileged populations. That is a review-workflow problem (screening terms, privilege-review passes, logs — see Guide 91), not a reason to leave a relevant custodian off the list.
- **Interview notes.** Custodian interviews conducted by lawyers for the dominant purpose of the litigation will usually attract litigation privilege (and legal advice privilege where the custodian is authorised to seek/receive advice for the client); mark and store them accordingly. The *existence* of sources they reveal is not privileged and feeds the DRD.
- **Confidentiality within the client.** Custodian data frequently contains material sensitive *inside* the organisation: HR issues, salaries, unrelated deals, board material. Restrict review-platform access by workspace and role, and agree internal protocols before collection — especially where the custodians include senior executives or HR staff.
- **Mixed personal content.** Corporate accounts contain personal messages; personal devices contain the reverse. Use targeted collection, search-term filtering and, for personal sources, an independent-examiner protocol so irrelevant personal material never reaches the review team (see §8.5 and §16).
- **Joint and common-interest complications.** Where a custodian served two group entities, or a director corresponded with lawyers for both a company and themselves, privilege may belong to someone who is not the disclosing party. Identify these situations in the interview and take advice before review, not after production.

16 UK GDPR and data minimisation

Collecting a custodian's mailbox is processing personal data — the custodian's and everyone else's in it. The UK GDPR and the Data Protection Act 2018 (as amended, including by the Data (Use and Access) Act 2025) apply throughout; disclosure obligations do not disapply them, but the framework accommodates litigation: establishing, exercising or defending legal claims is a recognised basis for processing (including for special-category data, DPA 2018 Sch 1 para 33), and legal-obligation and legitimate-interests grounds will usually support preservation and disclosure steps. What the framework demands is **discipline**, which happens to be the same discipline proportionality demands:

- **Minimise by design.** Tiering, per-custodian date ranges, source subsets and targeted collection (§7) are data-minimisation measures. Record them as such — the register doubles as your accountability documentation.
- **Tell custodians what is happening.** Transparency obligations point toward telling staff their data is being preserved and may be reviewed; a short privacy notice accompanying the hold notice is now standard good practice. (It also improves interview candour.)
- **Personal devices and accounts need extra care.** Voluntariness, a defined scope, an independent filtering process and prompt return/deletion of out-of-scope material — the *Phones 4U* pattern is also the UK GDPR pattern.
- **Special-category and third-party data.** Health matters in HR threads, family messages in mailboxes: plan redaction and access controls; do not let irrelevant sensitive data leak into productions.
- **Retention and disposal.** Collected custodian data should have an end-of-life: agreed retention through appeal windows, then certified deletion by the provider. Put it in the provider's instructions (§20, Wording D).
- **Overseas custodians.** International transfers for collection or hosting engage Chapter V; use providers with UK/EU hosting options or appropriate safeguards, and take local advice for custodians in restrictive jurisdictions (§8.6).

17 Common mistakes

Mistake	Consequence	Prevention
Building the list from today's org chart	Misses movers, leavers and the people who actually did the work in the relevant period	Period-specific org charts; HR joiners/movers/leavers report; interviews
Custodians only, no non-custodial sources	Shared mailboxes, repositories and systems never searched; incomplete DRD	Two-question rule (§5); IT interview before custodian interviews
No interviews ("we know who matters")	Personal chats, shadow IT and departed colleagues surface mid-review or at trial	Structured interview per custodian (§10), documented
Equating exclusion with non-preservation	Tier 3 name becomes central after their data was routinely deleted	Preserve the candidate list; collect the tiers (§7)
Leaver processes left running	Mailboxes and devices of departed custodians wiped on schedule, post-dispute	Day-one IT freeze; per-leaver status check (§8.1)
Ignoring PAs and delegates	The principal's real correspondence and filing lives with the assistant; attribution errors	Delegate questions in every interview (Group F)
Cross-custodian de-dup without custodian history	"Who held this document" becomes unanswerable	Require an all-custodians field; confirm production format (§14)
Agreeing opponent's custodian list without reasons	Disproportionate cost, or silent gaps on their side	

		Exchange reasoning; ask about their leavers and personal sources (§12.2)
No decision log	Methodology challenges met with reconstruction and hindsight	Live custodian and source register with dated decisions (§6)
Treating the list as final	Amendments, witness statements and EDA findings never fed back	Register review at every case milestone (§6, step 9)

18 Technical limitations

- **Accounts are not people.** Systems record account activity; linking an account to a human at a moment in time depends on authentication evidence, delegation records and sometimes forensic artefacts. Shared logins, kiosk machines and generic accounts may make individual attribution impossible.
- **Deleted leaver data may be genuinely gone.** Once retention windows and backup cycles have passed, no amount of ordering will retrieve a purged cloud mailbox. Alternative paths (counterpart mailboxes, archives, exports, printouts) are then the only paths — identify them rather than promising recovery.
- **Chat completeness varies by platform and licence.** What can be preserved and exported from Teams, Slack or WhatsApp depends on licence tiers, retention settings and platform APIs; edits, deletions, reactions and ephemeral modes may be partially visible or invisible. Ask the provider precisely what an export will and will not contain before relying on it (Guides 56, 63-66).
- **Personal-source collection depends on cooperation and technology.** A custodian's consent does not guarantee access (device encryption, app-level protections, cloud MFA), and extraction capabilities differ by device and OS version. Build time into the plan and manage expectations (Guides 61-62).
- **Mailbox conversions lose things.** Leaver mailboxes converted to shared mailboxes or exported to PST can lose folder-level metadata, dumpster content, or calendar/contacts data depending on method. What survives depends on steps taken by IT long before lawyers arrived — establish the history rather than assuming fidelity.
- **Interview memory is fallible.** Custodians forget accounts, underestimate personal-device use and misremember dates. Corroborate interviews against IT records (Group G), EDA communication maps and the documents themselves; treat contradictions as leads, not accusations.

19 Questions to ask the opponent and your provider

Questions for the client and its custodians are in §10. Two further banks complete the set.

Ask the opponent (in correspondence or at the DRD stage)

1. Which custodians (names and roles) do you propose to search, over what date ranges and which sources — and what was your basis for selecting them?
2. Which individuals involved in the events in issue have you excluded, and why?
3. Which relevant custodians have left your organisation? For each: what has happened to their mailbox, files, chat data and devices, and on what dates?
4. What steps have you taken to preserve custodian data — including suspension of deletion policies, JML freezes and device quarantine — and when?
5. Did relevant individuals use personal devices or accounts (including messaging apps) for the matters in issue, and what steps have you taken in respect of that material?
6. Which shared mailboxes, departmental repositories and systems of record will you search in addition to individual custodians?
7. What de-duplication approach will you apply, and will your productions preserve full custodian information for each document?

Ask the forensic / eDisclosure provider

1. For each custodian and source on our register, what collection method do you recommend, and what will it capture and miss?
2. How will you verify and document that each collection is complete and attributable (hashes, logs, chain of custody)?
3. Can you run early data assessment on Tier 1 to map communication patterns and test marginal custodians before we commit to full processing?
4. How does your platform record custodian metadata, and how is cross-custodian de-duplication handled — is an all-custodians field maintained and producible?
5. For leavers: what are the realistic recovery options per source (converted mailboxes, archives, backups, PST exports), and in what order should we try them?
6. For personal devices and accounts: what independent-examiner protocol do you offer, what filtering is applied, and who sees what at each stage?
7. Where will custodian data be hosted, who can access it, and what happens to it at the end of the matter (retention, return, certified deletion)?

20 Model wording

Adapt to the matter; none of this is a substitute for advice on the facts.

Wording A · Instruction to the client to convene custodian identification

> "To enable us to comply with the disclosure obligations that now apply, please arrange for us to speak with: (i) the person best placed to describe your IT systems, retention policies and leaver processes; (ii) the heads of the departments involved in [the events]; and (iii) the individuals listed in the attached schedule. Each conversation will take 30-60 minutes and will cover their role, communications, devices, accounts and document locations. Please do not ask anyone to gather, tidy or delete material in advance; the purpose is to find where documents are, and nothing should change until we have spoken. Please also tell us immediately of any listed individual who has left or is about to leave, so that their accounts and devices can be preserved today."

Wording B · Custodian paragraphs for a hold notice

> "You have been identified as a person who may hold documents relevant to [the dispute]. 'Documents' includes emails, chat and text messages (including WhatsApp and similar apps, on work or personal devices), documents and their drafts, spreadsheets, notes, calendars, voicemails and recordings, wherever stored — including personal devices and personal accounts if used for work. From now: (1) do not delete, alter or dispose of any such material; (2) switch off any disappearing-message settings in chats relating to [the matter]; (3) do not reset, replace, repair or return any device that may contain such material without first contacting [name]; (4) confirm by reply that you have read and will comply with this notice. If in doubt, keep it and ask."

Wording C · Proposing custodians to the opponent

> "Our client proposes to search the documents of the following custodians, whose roles and date ranges are set out in the enclosed schedule: [list]. These individuals were identified from the statements of case, interviews conducted with [n] members of staff, and analysis of communication patterns in an initial dataset. Our client will additionally search the following non-custodial sources: [shared mailboxes; repositories; systems]. We have preserved, but do not presently propose to search, the documents of [names/roles], for the reasons given in the schedule; our client will keep that position under review and invites your comments. Please provide the equivalent information for your client, including in respect of former employees and any relevant personal devices or accounts."

Wording D · Instructing the provider on custodian collections

> "Please collect, for each custodian listed in Schedule 1, the sources identified against their name, applying the date ranges stated. Collections are to be forensically sound and documented: for each, record custodian, source, method, tool and version, operator, date/time, scope applied and verification hashes, and maintain chain-of-custody records. Custodian attribution must be preserved through processing; apply global de-duplication only if all custodians holding each document remain recorded and reportable. Personal devices and accounts listed in Schedule 2 are to be handled under the independent-examiner protocol at Schedule 3 [scope; filtering; who sees what; return/deletion of out-of-scope material]. Host all data in [the UK/EEA]; at the conclusion of the matter, retain for [period] and then delete with certification. Report anything suggesting data loss, wiping or tampering immediately and before further processing."

21 Custodian identification checklist

- ☐ Issues extracted from statements of case and translated into events, actors, periods and systems
- ☐ Period-specific org charts, project lists and HR joiners/movers/leavers report obtained
- ☐ IT / organisational-knowledge interviews completed (systems, retention, JML, archives)
- ☐ Candidate custodian list assembled; custodian and source register opened
- ☐ Hold notices with privacy notice sent to all candidates; acknowledgements logged and chased
- ☐ Per-custodian IT preservation actions completed (mailbox/OneDrive holds, retention suspensions, device quarantine)
- ☐ Leavers: account status confirmed in writing; deletion timers frozen; archive/backup coverage checked
- ☐ Custodian interviews completed on the standard template; snowball names fed back into the register
- ☐ Personal-source use identified; preservation requests sent; independent-examiner protocol agreed where needed
- ☐ Shared mailboxes, departmental repositories, service accounts and systems of record listed as non-custodial sources
- ☐ Tiers assigned; inclusion/exclusion reasons recorded; sampling/EDA evidence filed for marginal decisions
- ☐ DRD Section 2 populated from the register (custodians, ranges, sources, unavailable data explained)
- ☐ Opponent's custodian list obtained with reasoning; their leavers and personal sources questioned
- ☐ De-duplication approach confirmed to preserve full custodian history
- ☐ Register reviewed at each milestone; holds re-verified before DRD certification and production

22 Red flags

TREAT ANY OF THESE AS A STOP-AND-ESCALATE SIGNAL

- A key actor resigned shortly before or after the dispute arose — and nobody has checked what happened to their account and devices.
- IT cannot say what the leaver process did to a named individual's mailbox, or the answer changes between askings.
- A custodian's interview answers conflict with system records (accounts or devices they "never used" show recent activity — or the reverse).
- Unexplained gaps: an obvious custodian has almost no documents for a critical period, or a thread's replies exist without the originals.
- A custodian "tidied up", ran a cleaner tool, or factory-reset a phone after the hold notice.
- Work was conducted in personal channels and the custodian is reluctant to discuss preservation of them.
- The opponent's custodian list omits the individuals your documents show at the centre of events, or refuses date ranges and reasons.
- Devices of departed custodians were reissued or recycled after litigation was in contemplation.
- Delegates or shared accounts sent key documents "as" a principal who denies knowledge.

Several of these fall within later guides on deleted evidence and destruction investigations (Guides 27-30). The immediate steps are always the same: preserve what remains, document the state of things as found, and take specialist advice before anyone touches the source again.

23 When to involve a digital forensic expert

Routine custodian collections from live corporate systems are eDisclosure work. Involve a digital forensic specialist when the custodian exercise itself raises questions only forensic methods can answer:

- **Leaver reconstruction.** Recovering or reconstructing a departed custodian's data from converted mailboxes, archives, backups, reissued devices or unallocated space — and evidencing what was lost, when and by what process.
- **Personal devices and accounts.** Acting as the independent examiner in a *Phones 4U*-style protocol: defensible extraction, filtering personal material, and reporting within an agreed scope.
- **Attribution disputes.** Establishing who used an account or device at the material time from authentication logs, artefacts and device evidence — including delegate-send and shared-login situations.
- **Suspected spoliation.** Any red flag in §22 involving deletion, wiping or resets after the duty to preserve arose: the examination must be forensically sound from the first touch, and the findings may ground (or rebut) applications and inferences.
- **Contested methodology.** Where the adequacy of a party's custodian identification or collection is challenged, an independent expert's report on method — and, where ordered, CPR Part 35 expert evidence — carries the argument. Guide 100 covers instructing experts, including Forensic Science Regulator Code compliance for criminal-justice work.

The economics favour early scoping: an hour's conversation with an examiner when the register is first drafted routinely prevents the expensive version of the same conversation a year later.

24 Scotland, Northern Ireland, arbitration, tribunals and criminal proceedings

Forum	How the custodian picture changes
Scotland	No PD57AD or DRD. Recovery of documents proceeds by commission and diligence, specification of documents and havers (third parties who hold documents). The practical discipline — identifying whose data matters and preserving it — is identical, but the vocabulary and procedure differ; "custodian lists" are a case-management practice rather than a rule-driven requirement.
Northern Ireland	Disclosure follows the Rules of the Court of Judicature (discovery by lists and affidavit, closer to pre-CPR practice). Commercial Hub judges expect parties to address electronic documents pragmatically; PD57AD-style custodian/DRD structures are useful as voluntary frameworks but are not mandated.
Arbitration	Document production is governed by the agreement, institutional rules and tribunal directions; the IBA Rules on the Taking of Evidence are the common reference. Custodian identification drives Redfern-schedule requests ("documents of X concerning Y between dates"), and tribunals expect proportionality; there is no DRD unless the tribunal adopts one.
Employment and other tribunals	Disclosure is ordered case-by-case (in ETs, by reference to CPR principles). Custodian counts are usually small, but personal devices and accounts loom larger — respondents should address BYOD and departed managers early, and claimants' own personal accounts are frequently in scope.
Criminal proceedings	Different regime entirely: CPIA 1996 disclosure turns on the prosecution's duty to pursue reasonable lines of enquiry and disclose material meeting the test, guided by the Attorney General's Guidelines (2024) and CPS policy. "Custodian" thinking maps to identifying devices, accounts and third-party material per suspect/witness; forensic work sits under the Forensic Science Regulator's statutory Code. Defence practitioners should probe the equivalent of custodian gaps in the prosecution's digital strategy.

25 Glossary

BYOD
Bring Your Own Device: personal hardware used for work, typically under a mobile device management policy.

Custodian
A person whose associated data sources are identified for preservation and possible search in disclosure.

Custodian interview
A structured, documented conversation establishing a custodian's role, habits, devices, accounts and document locations.

Custodian and source register
The working record of candidate custodians and sources, decisions, tiers, preservation status and reasons.

Delegate access
Rights allowing one user to act in another's mailbox or calendar; "send as" and "send on behalf" differ in the metadata they leave.

DRD
Disclosure Review Document: the PD57AD document in which parties set out Issues for Disclosure, models, custodians, sources and methodology.

Early data assessment (EDA)
Analysis of a dataset before full processing/review to estimate volumes, map communications and test custodian and search decisions.

Hold notice / legal hold
An instruction to custodians (and IT) to preserve potentially relevant material, with acknowledgement and follow-up.

JML
Joiners-movers-leavers: the HR/IT lifecycle whose leaver steps delete accounts and recycle devices on a timer.

Litigation hold (M365/Google)
A platform setting preserving mailbox/drive content, including deletions and edits, notwithstanding user actions or retention policies.

MDM
Mobile device management: software controlling enrolled devices, capable (dangerously, in this context) of remote wipe.

Model C / Model D
PD57AD Extended Disclosure models: request-led search-based disclosure (C) and issue-led search-based disclosure with or without narrative documents (D).

Non-custodial source
A repository not attributable to a single person: shared mailboxes, departmental repositories, systems of record, archives, backups.

PST
A Microsoft Outlook data file commonly used for mailbox exports; convenient but fragile and metadata-lossy if mishandled.

Service account
A non-human account used by systems, scripts or integrations; can hold and transmit documents without a human custodian.

Shared mailbox
A mailbox accessed by multiple users, typically functional (sales@, accounts@); attribution of items requires configuration knowledge.

Snowball sampling
Expanding the custodian list by asking each interviewee who else was involved, until no new names emerge.

Tiering

Ranking custodians by likely evidential value to phase collection and review effort proportionately.

26 References and further reading

- Practice Direction 57AD — Disclosure in the Business and Property Courts: justice.gov.uk/courts/procedure-rules/civil/rules/part-57a-business-and-property-courts/practice-direction-57ad
- Disclosure Review Document (with guidance notes): justice.gov.uk/documents/disclosure-review-document.pdf
- CPR Part 31 — Disclosure and Inspection of Documents: justice.gov.uk/courts/procedure-rules/civil/rules/part31
- Practice Direction 31B — Disclosure of Electronic Documents (including the Electronic Documents Questionnaire): justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b
- *Phones 4U Ltd v EE Ltd & Ors* [2021] EWCA Civ 116 (disclosure requests concerning custodians' personal devices and email accounts): bailii.org/ew/cases/EWCA/Civ/2021/116.html
- Review of Practice Direction 57AD — Disclosure Working Group survey summary (July 2026): judiciary.uk (PD57AD Working Party Summary, July 2026)
- Data Protection Act 2018: legislation.gov.uk/ukpga/2018/12/contents
- Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/18/contents
- ICO — Guide to the UK GDPR (lawful basis; data minimisation; individual rights): ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources
- Attorney General's Guidelines on Disclosure (2024) — criminal proceedings: gov.uk/government/publications/attorney-generals-guidelines-on-disclosure-2024
- Criminal Procedure and Investigations Act 1996: legislation.gov.uk/ukpga/1996/25/contents
- Forensic Science Regulator — Code of Practice (statutory): gov.uk/government/publications/forensic-science-regulator-code-of-practice
- SRA Standards and Regulations (competence and supervision in technology-dependent work): sra.org.uk/solicitors/standards-regulations
- This series: Guide 4 *Finding the Evidence* (source map and organisation-wide questionnaire); Guide 6 *Control of Electronic Documents*; Guides 21-30 (preservation and legal hold); Guides 61-70 (mobile and messaging sources).

Links were checked at the date of publication (September 2026). Court practice directions and government guidance move; verify the current version before relying on any of them.

27 How a specialist laboratory can assist

Much of this guide can be executed by a well-organised litigation team. A specialist UK electronic disclosure and digital forensic laboratory adds most value at the points where defensibility, recovery or independence are in play: scoping interviews alongside the legal team and translating them into a collection plan; forensically sound collection from corporate systems, devices and cloud platforms with full chain-of-custody documentation; acting as the independent examiner for personal devices and accounts under agreed protocols; early data assessment to test custodian and search decisions before costs are committed; reconstruction of leaver data from archives, backups and counterpart sources; and expert reporting where methodology or alleged spoliation becomes an issue, including CPR Part 35 evidence and, for criminal-justice work, engagements conducted with reference to the Forensic Science Regulator's statutory Code.

Computer Forensics Lab Ltd is a London-based digital forensics and eDisclosure laboratory working for law firms, in-house teams, investigators and private clients across the UK. Examiners work to forensic standards aligned with ISO 17025 practice, with secure UK evidence handling and courtroom-tested reporting. An early, no-obligation scoping conversation — before the custodian register is finalised — is usually the cheapest step in the entire exercise.

28 Disclaimer

This publication provides general information about electronic disclosure and digital forensics practice in England and Wales. It is not legal advice, nor advice on the facts of any matter, and it should not be relied upon as such. Procedural rules, guidance and technology change; positions stated here reflect the law and practice as understood at the date of publication (September 2026). Specific matters require advice from qualified lawyers and, where appropriate, qualified forensic practitioners instructed on the facts. No liability is accepted for reliance on this publication. Fictional examples (including Aldgate Components Ltd and Harlow Precision Engineering Ltd) are illustrative only; any resemblance to real entities or events is coincidental.

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