



Identifying the Right Custodians in Electronic Disclosure

Custodians and non-custodial sources; shared mailboxes, departmental repositories, service accounts, former employees and organisational data – how to choose the people whose documents get collected, defend the choices, and interview them so nothing surfaces late.

A practical guide for solicitors, barristers, litigation partners, associates, paralegals, in-house counsel, disclosure lawyers, investigators and litigation-support professionals · England & Wales, with notes for Scotland, Northern Ireland, arbitration, tribunals and criminal proceedings

Contents

Custodian selection decides most of a disclosure exercise's cost and most of its risk. This guide explains who should be on the list and why, how to grade and defend the list, how to interview the people on it, and how the list becomes the DRD – with the register, tiering model, decision tree and 40-question interview bank to do it.

1	Executive summary	3
2	The problem in plain English: people, not systems, drive cost	4
3	Why it matters legally: custodians in the rules and the cases	5
4	Important terminology	6
5	Custodial and non-custodial sources: two lists, one register	7
6	Who counts: roles and events, not ranks	8
7	The three-tier model: grading custodians by evidential weight	9
8	Special categories: leavers, assistants, service accounts, contractors, personal devices	10
9	The nine-step workflow: building the custodian and source register	11
10	Decision tree: include, tier, park or decline	12
11	The custodian interview: 40 questions in four parts	13
12	From register to DRD: drafting Section 2 custodian answers	15
13	Worked example 1: Aldgate's register – from 30 names to 9 custodians	16
14	Worked example 2: the hot custodian – Marsh from both sides of the litigation	17
15	Worked example 3: the sources with no owner – contracts@ and the GmbH	18
16	Privilege and confidentiality considerations	19
17	UK GDPR and data minimisation in custodian selection	20
18	Proportionality: the custodian count is the cost dial	21
19	Common mistakes and how to avoid them	22
20	Technical limitations lawyers should understand	23
21	Questions lawyers should ask their client	24
22	Questions lawyers should ask the opponent	25
23	Questions lawyers should ask a forensic or eDisclosure provider	26
24	Suggested wording for instructions and correspondence	27
25	Checklist: custodian selection essentials	28
26	Red flags	29
27	When to involve a digital forensic expert	30
28	How the rules differ: Scotland, NI, arbitration, tribunals, criminal	31
29	Glossary	32
30	Authoritative UK references	33
31	How a specialist laboratory can assist	34

Disclaimer. This publication provides general information about electronic disclosure and digital forensics practice in England and Wales. It is not legal advice and must not be relied on as such. The law, procedural rules and guidance change; always check the current versions and take advice on the facts of your matter. Case citations are provided for further reading. Computer Forensics Lab Ltd accepts no liability for reliance on this guide. © 2026 Computer Forensics Lab Ltd. Re-issued September 2026 in the series house style.

SECTION 1

Executive summary

After the issues themselves, no single decision shapes a disclosure exercise like the custodian list. Each name added multiplies gigabytes collected, documents processed and hours reviewed; each name wrongly omitted is a gap the opponent will find, and a reopened collection at triple the cost and none of the credibility. Yet custodian selection is often done in a meeting nobody minutes, on the basis of the org chart and a hunch.

This guide replaces the hunch with a method. It separates **custodial sources** (the data that follows people: mailboxes, OneDrives, phones) from **non-custodial sources** (the data that belongs to the organisation: shared mailboxes, repositories, systems) and puts both on one register. It selects people by **roles and events, not ranks**: the question is never "who is senior?" but "who touched the pleaded events?". It grades the list into **three tiers** – collect-and-review, collect-and-hold, monitor – so proportionality is built in rather than argued later. And it treats the **custodian interview** as the core diligence event of early disclosure: forty questions that surface devices, apps, personal accounts, deletion habits and the documents people would rather explain than have found.

The output is a **custodian and source register**: one versioned document recording, for every person and source, the connection to the issues, the tier, the sources held, the interview date, the preservation status and the inclusion decision with reasons. The register drives the litigation hold (Guide 22), populates DRD Section 2 (Guide 15), prices the proportionality argument (Guide 8's EDA consumed it), and is the exhibit that answers "why these custodians?" at the CMC.

THE GUIDE IN ONE PARAGRAPH

List generously, interview systematically, tier ruthlessly, record everything. A register of 30 names with 9 in Tier 1 is cheaper and more defensible than a list of 15 assembled by seniority – because the 21 declined or parked names carry dated reasons, and the 9 collected ones carry interviews proving the choice was informed.

SECTION 2

The problem in plain English: people, not systems, drive cost

Guide 4 mapped where evidence lives. This guide answers the harder question: *whose* evidence do you actually take? The difficulty is structural:

- **Modern data is person-shaped.** Cloud platforms organise everything around accounts: a mailbox, a OneDrive, a Teams identity per person. Selecting custodians *is* selecting data volume – in the series case, each Aldgate custodian averaged roughly 45 GB before culling.
- **Relevance does not follow the org chart.** The CEO "was across everything" and holds almost nothing unique; the operations manager who wrote the candid emails is two levels down. Seniority-driven lists collect the wrong gigabytes.
- **The obvious list is always incomplete.** Assistants sending in their principal's name; the leaver whose account is mid-deletion; the contractor on a personal laptop; the shared mailbox nobody owns. The people who know these exist are the custodians themselves – which is why interviews, not meetings, build the list.
- **Every name is a negotiation.** The opponent will propose custodians you consider marginal, and challenge omissions you consider obvious. Without a register with reasons, both conversations are assertion against assertion (Guide 17 covers the negotiation itself).

THE TWO FAILURE MODES

Too many custodians: review costs balloon and the budget is spent on duplicates of documents Tier 1 already held (deduplication mitigates but does not cure – processing and hosting still cost). Too few: the gap surfaces in the opponent's cross-referencing ("why is Ms Devlin cc'd on every disclosed email but not a custodian?"), and the late addition costs more than the early one ever would have – plus the credibility.

SECTION 3

Why it matters legally: custodians in the rules and the cases

- **PD 57AD and the DRD.** The Disclosure Review Document requires each party to identify the custodians whose documents will be searched, with date ranges, and to explain excluded categories. Paragraph 3.2's legal-representative duties include taking reasonable steps to ensure the client identifies where relevant documents are held – whose accounts, not just which systems. The preservation duty (paras 3.1, 4.2) expressly extends to relevant documents of **former employees**, and paragraph 4's machinery includes notifying them.
- **Reasonable search.** Custodian scope is the first of the classic reasonable-search dimensions (Guide 7). *Digicel (St Lucia) v Cable & Wireless* [2008] EWHC 2522 (Ch) ordered searches of additional custodians the defendants had unilaterally excluded; the modern equivalent is the court resolving a disputed DRD custodian schedule at the CMC – on evidence about roles, which the register provides.
- **Personal devices and accounts.** *Phones 4U Ltd v EE Ltd* [2021] EWCA Civ 116 confirmed the court's power to require a party to ask employees and former employees to produce work-related material on personal devices and accounts, with appropriate privacy safeguards. Custodian analysis therefore cannot stop at corporate sources: the question "does this custodian's business traffic live anywhere personal?" is a legal requirement, not curiosity (see the interview bank, Part C).
- **Known adverse documents.** The paragraph 3.1(2) duty operates through people: a company "knows" what its accountable individuals know (Guide 16's attribution analysis). Custodian selection and the certificate exercise are the same inquiry at different moments – omit the person who knows about the adverse thread and the certificate is built on sand.
- **Costs.** Custodian disputes are resolved by proportionality arithmetic (para 6.4), and the party whose tiered register carries volumes and costs per name wins those arguments; the one defending a seniority list does not.

SECTION 4

Important terminology

Term	Meaning
Custodian	A person whose documents and communications are preserved and (if pursued) collected: their mailbox, files, devices and app data.
Non-custodial source	Organisational data not owned by one person: shared mailboxes, departmental repositories, line-of-business systems, logs.
Custodian and source register	The versioned document recording every candidate person and source, their issue-connection, tier, holdings, interview status and inclusion decision with reasons.
Tiering	Grading custodians by evidential weight into collect-and-review / collect-and-hold / monitor (Section 7).
Shared / role mailbox	A mailbox addressed to a function (contracts@, sales@) used by several people; high-value, frequently orphaned.
Service account	A non-human account used by systems or integrations; occasionally relevant (automated reports, scanner-to-email chains).
Leaver / former employee	A departed person whose data may survive in preserved accounts, archived mailboxes, backups or reissued devices – expressly within the preservation duty.
Delegate access	One person operating inside another's mailbox or files (assistants); breaks naive one-person-one-account assumptions.
De-duplication	Suppressing identical documents across custodians at processing; makes overlapping custodians cheaper to review but not free to collect and host.
BYOD	Business data on personal devices; a custodian attribute that changes the collection plan and the legal route (see <i>Phones 4U</i>).

SECTION 5

Custodial and non-custodial sources: two lists, one register

The register has two halves because evidence has two owners:

5.1 The custodial half

People, each with their source bundle: mailbox (live or archived), personal cloud store (OneDrive/Drive), device set (laptop, phone, tablet, and their predecessors), chat identity (Teams/Slack DMs), and any personal-account or BYOD exposure. The bundle travels with the person: adding a custodian means adding the whole bundle to the preservation scope, even if only part is later collected.

5.2 The non-custodial half

Sources that would vanish from a people-only view: shared and role mailboxes; departmental shares and SharePoint sites; DMS libraries; line-of-business systems (CRM, ERP, accounting); logs and audit trails; and physical stores. Each needs a named **steward** – not an owner in the custodial sense, but the person who can answer questions about it and authorise its preservation.

WHY ONE REGISTER, NOT TWO LISTS

Because the halves cross-populate: custodian interviews surface non-custodial sources ("we ran all tenders through contracts@"), and non-custodial sources nominate custodians (the CRM's activity log shows who actually worked the account). A register that holds both, with links between them, is how the surprise mailbox and the surprise author are both avoided.

SECTION 6

Who counts: roles and events, not ranks

Build the candidate list from the pleaded events outward:

1. **Event mapping.** For each Issue for Disclosure (or pre-action equivalent), list the events that will prove or rebut it: the negotiation meetings, the price changes, the deliveries, the complaints, the departure. Guide 13's documents-first anatomy works in both directions.
2. **Actor extraction.** For each event: who did it, who wrote about it, who was told, who decided? Sources: the documents already held, correspondence signature blocks, meeting invites, CRM activity, and the client team's memory – cross-checked, because memory nominates the senior and forgets the operational.
3. **Role classes to check deliberately** (the reliably forgotten): deal-doers' *deputies* who drafted what principals signed; assistants with delegate access; finance staff who processed the disputed numbers; engineers and technical staff whose files are the subject matter (the series' A. Szabo, CAD custodian); complaint-handlers; and everyone who *left* during the relevant period.
4. **Communication analysis.** Once any data is processed, let it talk: sender/recipient frequency across the issues' date ranges shows who actually corresponded about the events. Guide 8's EDA does this cheaply and often re-ranks the list – the loudest correspondent is sometimes a name no meeting suggested.

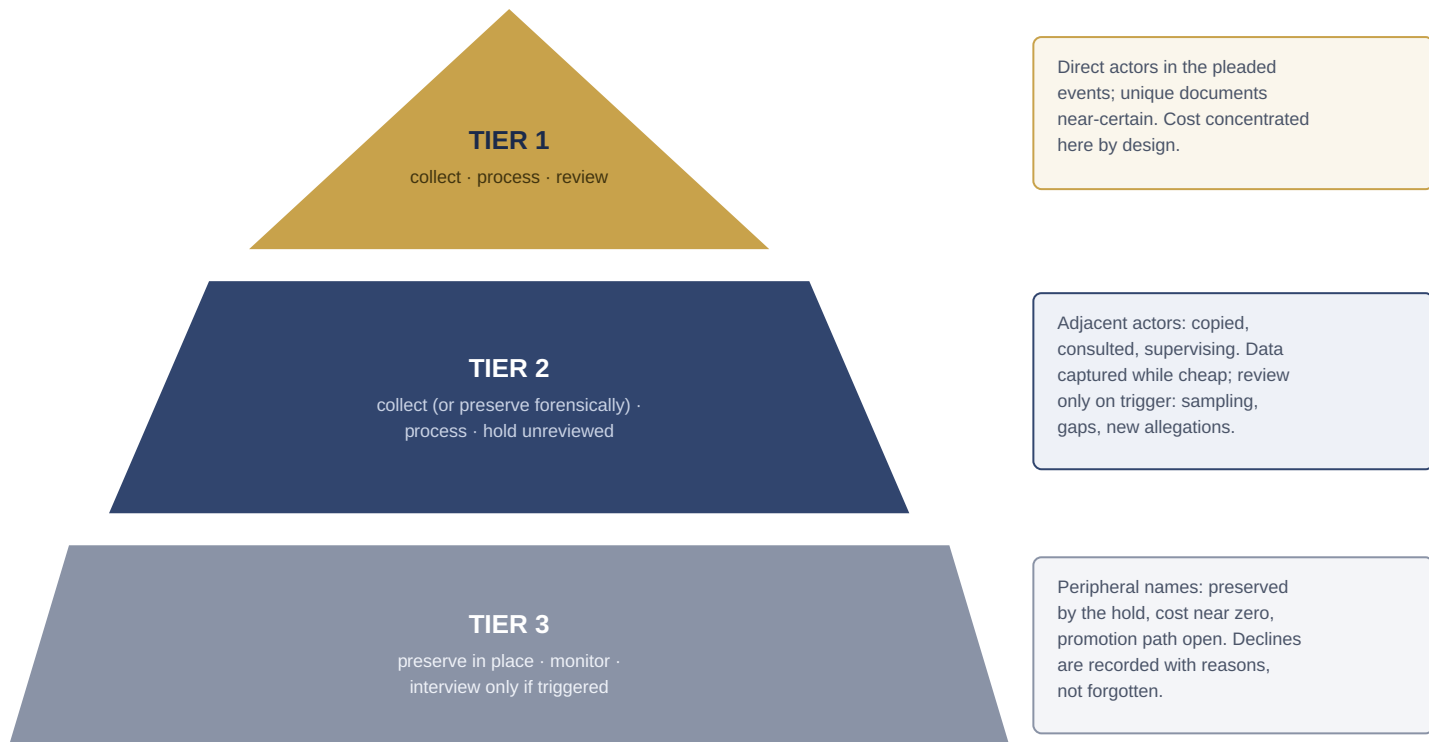
Rank is a proxy for authority, not for evidence. Include senior people when they *acted* (signed, decided, was warned), not because omission feels impolite. The most expensive custodian in most registers is the courtesy inclusion.

SECTION 7

The three-tier model: grading custodians by evidential weight

Binary lists (in/out) force every marginal name into a fight. Tiering converts the fight into a dial – Figure 1.

Figure 1 · The three-tier custodian model: proportionality built into the list



Movement between tiers is the register's normal life: EDA re-ranks, sampling promotes, interviews demote. What never moves silently is the record – every tier change carries a date and a reason.

The tiers price differently: Tier 1 carries full collection, processing and review; Tier 2 carries collection and processing only (cheap insurance against reopened collections – the data is banked while devices exist and accounts live); Tier 3 costs a hold-notice entry. In negotiations (Guide 17) tiers are the natural counter-offer: "we will not review your six marginal names, but we will collect and hold three of them, promotion on sampled evidence."

SECTION 8

Special categories: leavers, assistants, service accounts, contractors, personal devices

8.1 Former employees

The highest-risk category, because their data is on deletion clocks and their cooperation is optional. PD 57AD's preservation machinery expressly reaches them: paragraph 4.2 contemplates written notification to relevant former employees, and Guide 16's certificate practice showed the polite-but-necessary paragraph 2.9 leaver letter in action (Marsh, via Harlow's solicitors: nothing returned, dispatch logged). Register practice: leavers are custodians like any other, with an extra column – what survives (account? archive? backups? reissued device?) and what the leaver process destroyed, with dates. The Marsh row is the series' worked example (Section 14).

8.2 Assistants and delegates

Anyone with delegate access to a Tier 1 mailbox or diary effectively *is* part of that custodian's data – and has their own bundle besides. Ask the delegation question in every interview (bank Q14): assistants know about side channels ("he always had me print the sensitive ones") that principals forget to mention.

8.3 Shared and role mailboxes, service accounts

Non-custodial but decisive: tenders, complaints and orders route through them, and no individual's collection captures them. Each needs a steward, a preservation entry and a tier of its own. Service accounts matter when workflows emailed reports or scanned documents into the record – occasionally the only copy of a disputed attachment.

8.4 Contractors, consultants and secondees

Their data may sit on your client's tenancy (easy), their own company's (a control question: Guide 6), or personal equipment (a *Phones 4U* question). The contract's IP, confidentiality and audit clauses decide the route; the register records which regime each contractor falls under, so no one discovers at collection that the key designer's files live on his own NAS.

8.5 Personal devices and accounts

Phones 4U v EE [2021] EWCA Civ 116: the court can require a party to **ask** employees and former employees to hand over or permit search of work material on personal devices and accounts, with privacy protections; refusal has consequences the court manages case by case. Register practice: BYOD exposure is an attribute of every custodian (interview Part C), and collection from personal sources is targeted, documented and privacy-screened – the series' Q2 2027 BYOD tier (three bid-team phones, defined scopes) is the shape (Guide 68 will treat BYOD in full).

THE QUIET DESTRUCTION EVENT

Most custodian-related evidence loss is not misconduct; it is the leaver process running as designed. The register exists partly so that one page – leavers, with dates and what survives – can be checked against the hold on day one. In the series case that check is why Marsh's laptop image existed (quarantined before confrontation) while his phone did not (wiped on departure, ten months before solicitors were instructed – a fact disclosed early, with its dates, rather than discovered late).

SECTION 9

The nine-step workflow: building the custodian and source register

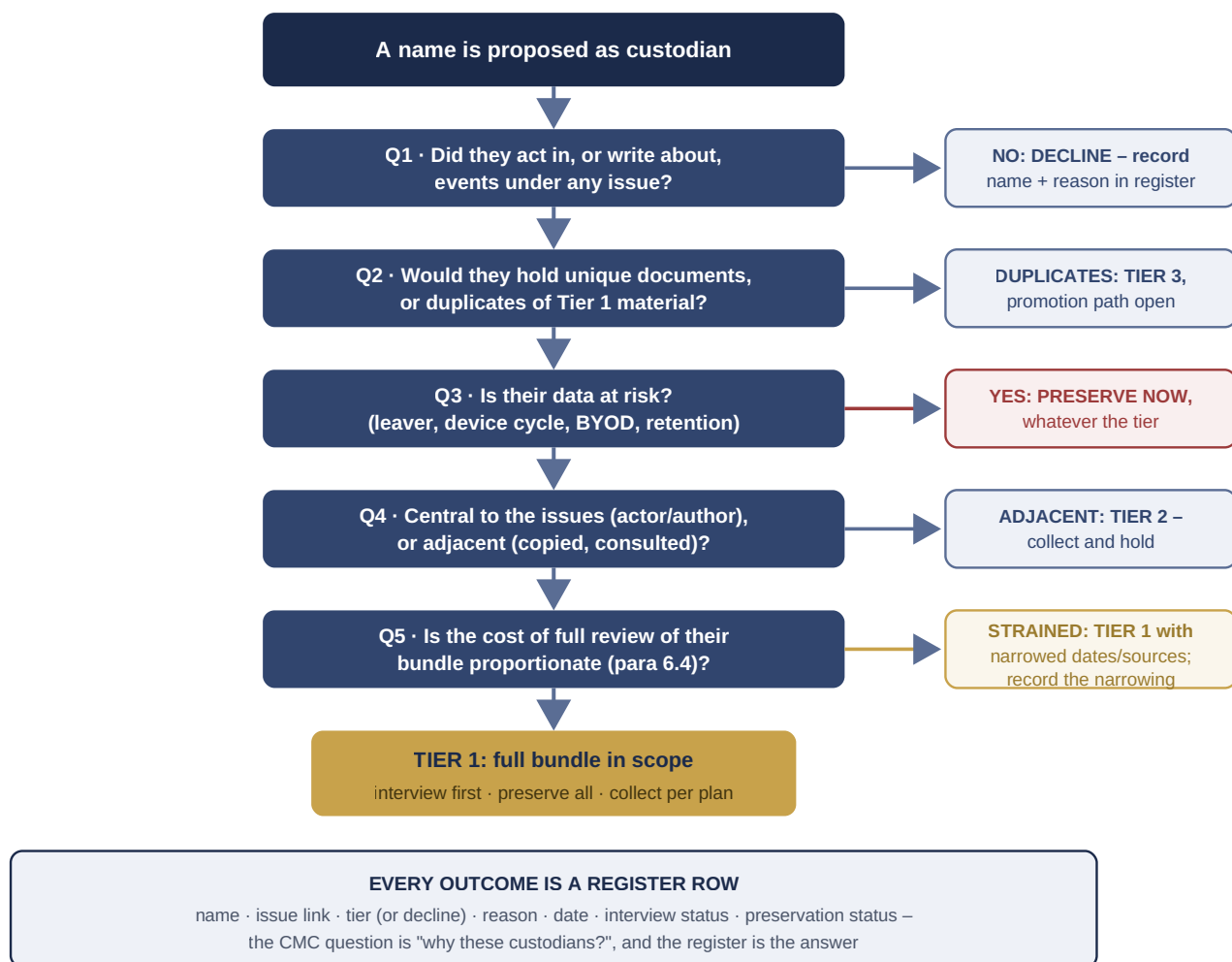
#	Step	How	Output
1	Frame issues and events	Pleadings/correspondence → event list per issue (Section 6.1)	Event map
2	Extract candidate actors	Documents held, signature blocks, invites, CRM activity, client memory – generously	Candidate list (long)
3	Add the forgotten classes	Deputies, assistants, finance, technical staff, complaint handlers, leavers, contractors	Candidate list (complete)
4	Attach non-custodial sources	From the data map (Guide 4): shared mailboxes, repositories, systems, each with steward	Register skeleton
5	Interview	Section 11's 40 questions; Tier 1 candidates first; note verbatim; verified-vs-assumed marking	Interview records
6	Tier	Figure 1 model, applied per issue; volumes and costs estimated per name (provider assists)	Tiered register v1
7	Preserve accordingly	Hold notices (Guide 22), leaver freezes, device quarantine, BYOD instructions	Preservation log entries
8	Validate with data	EDA communication analysis re-ranks; sampling tests marginal names (Guide 8)	Register v2 + change log
9	Publish and maintain	DRD Section 2 custodian schedule from the register; updates as issues sharpen	DRD entries; living register

In the series case the register ran from the 23 January 2026 scoping to **v4 by the DRD phase** (Guide 15), its change log recording each addition and demotion – including one interview-driven addition nobody's memory produced: the finance analyst whose margin reports turned out to be the pricing issue's paper trail.

SECTION 10

Decision tree: include, tier, park or decline

Figure 2 · Custodian triage: from candidate name to recorded decision



Q3 cuts across the tree on purpose: preservation is decided by risk, not importance. A Tier 3 leaver's account gets frozen today; whether anyone ever reviews it is a different, later decision.

SECTION 11

The custodian interview: 40 questions in four parts

Interview Tier 1 candidates before finalising anything: the interview is where the register earns its keep. Tone matters – this is diligence, not cross-examination; people who feel accused forget things, and people who feel helped remember the WhatsApp group. Note answers verbatim where they matter, and mark each material answer verified (checked against a system) or assumed (their say-so) per Guide 10's discipline.

Part A · Role and events (9)

1. Walk me through your role in [the events], start to finish.
2. Which of these events did you act in personally – decide, sign, send, build, deliver?
3. Who did you work with most closely on them, inside and outside the company?
4. Who else saw or was told about the key exchanges at the time?
5. What meetings mattered, and were they minuted, recorded or diarised?
6. Which issue-relevant documents did you author or receive first-hand?
7. Where would you look tonight for the most important document on this?
8. Who has left the company who was involved – and what did they hold?
9. Who am I not asking about that I should be?

Part B · Systems and habits (11)

1. Which devices do you use for work – issued and personal, current and previous?
2. Where do your files live: local, OneDrive/Drive, shares, DMS, anywhere else?
3. How do you use email: folders, archiving, auto-delete habits, local PSTs?
4. Which chat tools carry your work conversations – Teams/Slack channels, DMs, group chats?
5. Does anyone have delegate access to your mailbox, diary or files? Do you have it to anyone's?
6. Which business systems do you work in daily (CRM, ERP, finance, ticketing), under what login?
7. What do you keep on USB sticks or external drives?
8. Do you print and keep paper, or keep notebooks, for anything relevant?
9. Any recordings: calls, meetings, voice notes, dictation?
10. What shared mailboxes or team resources do you use for this work?
11. If you needed to send something too sensitive for email, how would you send it?

Part C · Personal-channel exposure (10)

1. Do you ever use personal email for work – forwarding, sending, receiving? Examples, not policy.
2. Which messaging apps on your personal phone carry work traffic (WhatsApp, Signal, SMS, others)?
3. Which work-related groups are you in on those apps, and who else is in them?
4. Are disappearing messages on in any of them? Since when?
5. Do you sync work files to personal cloud accounts (Dropbox, iCloud, Google)?
6. What happened to your previous personal phone?
7. Do you use a home computer for work – and does it sync or store anything?
8. Would you be willing to let us collect the work-related material from personal sources under a privacy-protecting protocol? (Explain *Phones 4U* obligations plainly.)
9. Social media: any work-relevant contact with counterparties or competitors through it?
10. Is there anything on a personal channel you would rather tell us about now than have found later?

Part D · Preservation and conduct (10)

1. Have you received and read the hold notice? Any questions about it?
2. Have you deleted, archived or tidied anything relevant since the dispute arose?
3. Has anyone asked or suggested you delete, move or withhold anything?
4. Any auto-delete rules, mailbox cleanup habits or full-mailbox pressures we should suspend?
5. Any devices due for replacement, repair or return we should intercept?
6. Are you aware of documents adverse to us on these issues? (Known-adverse duty, Guide 16 – asked plainly and without drama.)
7. Are there documents that would embarrass you personally that we should discuss privately? (Privilege and welfare handling as appropriate.)
8. Who else should hear this interview's questions?
9. Will you tell us if you remember something later – and do you know who to tell?
10. Anything else we should have asked?

SECTION 12

From register to DRD: drafting Section 2 custodian answers

The DRD's custodian questions (Guide 15 maps the form in full) are the register, filtered for publication:

- **Publish:** names (or roles, where names are sensitive), date ranges per issue, the source types per custodian, and the fact of tiering with its promotion triggers. This is the Guide 17 left lane: methodology, offered with numbers.
- **Hold back:** interview contents, work-product observations, and the reasons that reveal strategy (a decline reasoned "peripheral to events" publishes; one reasoned "his emails help us and we will deploy them at trial" does not – and should not exist in the publishable layer anyway).
- **Reconcile before filing:** the register's change log against the DRD draft, so the schedule filed 14 January (in the series timeline) matches what interviews and EDA actually established – discrepancies between early correspondence and the DRD are the opponent's favourite cross-reference.
- **Expect negotiation:** the opponent's additions are tested by the Figure 2 tree with numbers attached (Guide 17's tiered-offer tactic); your refusals carry the register's reasons.

THE Q8 HABIT

Where a custodian's data has a known defect – the series' example: Marsh's mailbox gap, November 2024 to March 2025 – the register is where it is first recorded, and the DRD's honesty questions (the Guide 15 Q8 row) are where it is disclosed, with the recovery steps taken. Custodian defects disclosed early with dates are case management; discovered late they are conduct allegations.

SECTION 13

Worked example 1: Aldgate's register – from 30 names to 9 custodians

ALDGATE COMPONENTS LTD v HARLOW PRECISION ENGINEERING LTD · THE SERIES CASE STUDY

Aldgate disputes Harlow's termination of their supply agreement and alleges misuse of confidential pricing and CAD theft by ex-commercial director James Marsh (departed 21 March 2025, joined Harlow). First scoping meeting: 23 January 2026. Data map signed off 30 January (Guide 4); hold complete 4 February.

Step 2-3 (candidates). Event mapping across the eventual five issues produced 30 names: the commercial team, operations, engineering, finance, the GC's office, two assistants, three leavers including Marsh, and two contractors.

Step 5 (interviews). Eleven interviews in the first three weeks. Yields beyond confirmation: the finance analyst whose margin reports documented the pricing methodology (added – no meeting had named her); the operations manager P. Devlin's candid delivery correspondence (his centrality was already suspected; the interview confirmed his habits – email, minimal chat); engineering custodian A. Szabo's CAD vault knowledge (fixing the folder structure and access-log capability that became Issue 3's Model C request); and the sales team's WhatsApp group (three members, preserved accordingly).

Step 6 (tiering). Register v1: **9 Tier 1** (Marsh's surviving bundle; R. Okafor, sales director; Devlin; Szabo; the finance analyst; the commercial manager who inherited Marsh's accounts; the GC for defined threads; two bid-team members), **7 Tier 2** (adjacent commercial and operations staff; both assistants), **14 Tier 3** (declined-for-now with reasons: peripheral, duplicative, or events outside the ranges). Non-custodial half: *contracts@* (steward: commercial manager), the CAD vault, the ERP order tables, Purview audit exports, Veeam sets.

Step 8 (validation). The Guide 8 EDA re-ranked twice: one Tier 2 assistant promoted (delegate-sent traffic in Marsh's name), one Tier 1 bid-team member demoted to Tier 2 (nothing unique after dedupe). Register v4 stood behind the DRD schedule filed 14 January 2027; the court's custodian questions at the 21 January CMC were answered from it in minutes.

THE ARITHMETIC THAT HELD

Nine reviewed custodians, averaging ~45 GB raw each, fed the 412 GB / 2.81m item collection that EDA culled 44% by deduplication toward the 61,400-document review population (Guide 8's canonical figures). Every downstream number the proportionality arguments used traces to the tier decisions made here – which is why the register, not the review platform, is where cost control actually happens.

SECTION 14

Worked example 2: the hot custodian – Marsh from both sides of the litigation

As Aldgate's former employee, Marsh is a leaver-custodian with a defect schedule: mailbox preserved but with the November 2024-March 2025 sent-items gap; laptop imaged (quarantined before confrontation); phone wiped and reissued on departure; OneDrive intact; personal-Gmail exposure suspected at registration, confirmed at the Guide 16 certificate interviews (40 forwards). Register practice on display: every defect carries dates, the recovery paths (audit logs, recipients' copies, Veeam monthly snapshots), and the disclosure route (DRD Q8 entry).

As Harlow's current employee, Marsh is the opponent's accountable custodian: his awareness attributes to Harlow for known-adverse purposes (Guide 16), his Harlow mailbox was held for the CMC and returned as a targeted Model C class (Guide 15), and his onboarding – Harlow instructed independent forensics when hiring him – became Harlow's best conduct evidence. The lesson for any party hiring from a dispute counterparty: the incoming person is a future custodian; onboard accordingly, with imaging, undertakings and segregation, because the register you will someday defend starts on their first day.

Preservation sequencing (Guide 2's preserve-examine-confront): Aldgate imaged the laptop *before* confronting Marsh, so the artefact record (USB connections, uploads) predates any opportunity for reactive tidying. Custodian handling and forensic sequencing are the same discipline seen from two chairs.

SECTION 15

Worked example 3: the sources with no owner – contracts@ and the GmbH

The shared mailbox. Aldgate's tenders and counterparty negotiations routed through *contracts@* – used by four people across the relevant period, owned by none. A people-only list would never have collected it; the register's non-custodial half carried it as a source with the commercial manager as steward, its own date ranges, and its own DRD line. At review it held the only complete thread of one disputed tender – individual custodians had deleted their copies in ordinary mailbox hygiene.

The group company. A procurement manager at **Aldgate Manufacturing GmbH** held relevant supplier correspondence (Guide 6 analysed the control question: subsidiary data, parent litigation). Register practice: he appears as a custodian with a jurisdiction flag – German employment law and GDPR shape the collection route, timing and consent process (Guide 40 will cover multi-country collection). The flag prevented the classic error: a UK-drafted hold notice sent to a German employee without works-council consideration, surfacing months later as a procedural complaint.

STEWARDSHIP IN ONE LINE

Every non-custodial source needs a human name beside it – not as owner but as answerable: who can describe it, freeze it, and authorise its export. A source without a steward is a question with no addressee, and it will be asked at the worst possible time.

SECTION 16

Privilege and confidentiality considerations

- **Interviews.** Custodian interviews conducted for the litigation attract litigation privilege; keep the dominant purpose visible in how they are commissioned and recorded. For legal advice privilege, remember the *Three Rivers (No 5)* client-team limits in corporate settings: structure interview records as litigation-privilege work product, not as "client communications" assumptions.
- **The register's two layers.** Like Guide 17's decision log: an exhibitable layer (names, tiers, dates, published reasons) and a privileged layer (interview substance, strategy-revealing reasoning). Draft rows knowing the first layer may be shown to a judge.
- **Custodians with privileged bundles.** The GC and anyone in the advice chain need quarantine workflows before collection (screening protocols, privilege terms in the review plan) – flag on the register so processing is configured before their data lands.
- **Employee-interest conflicts.** Interview answers can implicate the custodian personally (Part D questions). Have the separate-representation conversation ready, and never trade a custodian's candour for a welfare or conflicts problem later.
- **Confidential personal content.** BYOD and personal-account collection must screen private material away from the legal team by protocol – both a GDPR matter (Section 17) and the practical price of custodian cooperation.

SECTION 17

UK GDPR and data minimisation in custodian selection

- **Tiering is minimisation.** Article 5(1)(c) UK GDPR (unchanged in substance by the Data (Use and Access) Act 2025 amendments) asks for no more personal data than the purpose requires; the three-tier model operationalises exactly that, and documents it.
- **Lawful basis.** Legitimate interests (with a recorded balancing test) is the usual basis for processing employee data in disclosure; consent is generally inappropriate in employment settings. Transparency duties are met through hold notices and, where appropriate, privacy-notice updates.
- **Personal channels.** *Phones 4U*-style requests are targeted asks, not device seizures: defined scopes, custodian-assisted or examiner-mediated extraction, private material screened out before legal review (the series' three-phone BYOD tier is the template).
- **Leavers.** Processing former employees' data is expected by the preservation rules; keep the scope issue-led and the retention linked to the proceedings.
- **Cross-border custodians.** The GmbH flag: EU-based custodians bring EU GDPR, works councils and local employment law into the route; plan transfers and consultation before collecting, not after.
- **Records.** The register plus preservation log is the accountability record; date both, version both.

SECTION 18

Proportionality: the custodian count is the cost dial

Disclosure cost scales roughly linearly with reviewed custodians – before dedupe efficiencies, each Tier 1 name in the series case represented on the order of tens of gigabytes collected and thousands of review documents. Paragraph 6.4's factors are therefore argued most concretely at the custodian line: probative likelihood per name, volumes per name, cost per name.

The register makes the argument mechanical: "our nine reviewed custodians cover every actor in the pleaded events; your six proposed additions are copied-in adjacents whose unique-document yield, tested by deduplication against Tier 1 collections, was below [x]% in sampling; we offer Tier 2 treatment for three." That sentence – the Guide 17 tiered offer – wins CMC minutes because every clause carries a number the register generated.

DATE RANGES ARE HALF THE DIAL

Custodian cost = names × ranges × sources. Narrowing a marginal custodian to the four months they touched the events is often the agreement that avoids the fight about excluding them entirely – and per-issue ranges (Guide 4, Section 7.1) do it defensibly.

SECTION 19

Common mistakes and how to avoid them

Mistake	Consequence	Fix
Selecting by seniority	Expensive duplicates in; unique authors out	Roles-and-events method (Section 6)
Skipping interviews for "obvious" custodians	Personal channels, delegates and habits missed; certificate surprises later	40-question bank for every Tier 1 name
People-only lists	Shared mailboxes and systems never collected	Non-custodial half with stewards (Section 5)
Leavers handled last	Deletion clocks beat the hold	Leaver freeze day one; defect schedule per leaver
Binary in/out lists	Every marginal name becomes a dispute	Three tiers with promotion triggers
No recorded reasons for declines	"Why not Ms X?" answered by silence at the CMC	Register rows for declines too
Ignoring the data's own evidence	List reflects memory, not traffic	EDA communication analysis re-ranks (step 8)
BYOD ignored until collection	<i>Phones 4U</i> obligations discovered under deadline	Part C questions at interview; protocol early
Register diverges from DRD	Opponent cross-references the inconsistency	Reconcile change log before filing (Section 12)
Register unmaintained after CMC	New issues meet a stale list	Named owner; review at every phase gate

SECTION 20

Technical limitations lawyers should understand

- **Accounts are not people.** Delegates, shared logins and service accounts mean the mailbox's "sender" is a hypothesis, not a fact; attribution needs corroboration (authentication logs, style, devices) when it matters (Guide 41 onward).
- **Deduplication is scoped.** "Adds nothing unique" claims depend on dedupe scope (global vs per-custodian) and order; ask the provider how uniqueness was computed before deploying the number in negotiation.
- **Leaver survival varies by platform and licence.** What remains of a departed custodian (retained mailbox? archived? gone at 30 days?) is configuration-specific; verify in the console per leaver, never assume from policy.
- **Communication analysis sees what was collected.** EDA re-ranking works on processed sources; a custodian whose real traffic ran on WhatsApp looks quiet in an email-only analysis – interviews catch what analytics cannot.
- **Personal-source collection has limits.** Extraction from personal devices depends on device, OS and cooperation; some app data is retrievable only with the custodian's active participation (Guide 61-65 territory). Build cooperation, not just compulsion, into the plan.
- **Historic bundles fragment.** A 2019-era custodian's data may be spread across a migrated tenancy, an old archive and a backup format two vendors ago; per-custodian source completeness is a verification task, not a checkbox.

SECTION 21

Questions lawyers should ask their client

1. Who, by name and role, acted in each of the events we will have to prove or rebut – and who drafted what the actors signed?
2. Who has left since the events, when, and what happened to their accounts and devices under your leaver process?
3. Which assistants, deputies or delegates worked inside the key people's mailboxes and diaries?
4. What shared mailboxes, team addresses or departmental repositories carried this work, and who can speak for each?
5. Which contractors, consultants or secondees touched the events, and under what contracts and equipment arrangements?
6. Which group companies or overseas offices hold relevant people, and what local-law constraints apply to reaching their data?
7. Whose work habits run through personal phones, personal email or home computers – honestly?
8. Who is likely to hold documents adverse to us, and who knows about them? (The Guide 16 duty starts here.)
9. Which of these people face device refreshes, departures or restructuring in the next six months?
10. Who will own the register internally and warrant its accuracy at sign-off?

SECTION 22

Questions lawyers should ask the opponent

1. Who are your proposed custodians, with roles, employment dates and date ranges per issue – and on what basis was each selected?
2. Which individuals involved in the events are *not* proposed, and why?
3. What former employees held relevant roles; what survives of their data; and when did their accounts and devices enter your leaver process?
4. What shared or role mailboxes, departmental repositories and systems carried the relevant work, and are they within your proposed sources?
5. Which custodians had delegate or assistant access arrangements?
6. What steps have you taken regarding work material on custodians' personal devices and accounts (*Phones 4U*)?
7. What preservation notices have been given to current and former employees, and when?
8. For any custodian whose data has known defects (gaps, wiped devices, deleted accounts), what are the specifics, dates and recovery steps?
9. Will you provide per-custodian volume estimates so proportionality can be discussed on numbers?
10. Will you agree a tiered treatment (collect-and-hold with promotion triggers) for the custodians we each consider marginal?

SECTION 23

Questions lawyers should ask a forensic or eDisclosure provider

1. Can you produce per-custodian volume and cost estimates from the tenancy before we finalise tiers?
2. How will you verify each custodian's actual source bundle (consoles, asset registers) rather than relying on interview answers alone?
3. What survives of each named leaver, verified per platform – and how fast can leaver freezes take effect?
4. How do you run communication analysis for list validation, and across which collected sources?
5. What is your dedupe scope and uniqueness methodology, so tier arguments carry defensible numbers?
6. What is your protocol for personal-device and personal-account collection: targeting, custodian assistance, privacy screening, documentation?
7. How do you preserve and collect shared mailboxes and delegate-access situations so attribution survives?
8. Can you support interviews with a technical attendee, and produce verified/assumed annotations against systems?
9. What does Tier 2 (collect-and-hold) cost per custodian versus Tier 1, so the tiered offer is priced?
10. Which custodians' situations need forensic handling now (imaging before confrontation, defect documentation) rather than standard collection later?

SECTION 24

Suggested wording for instructions and correspondence

A · LEAVER FREEZE (to client IT, day one)

"With immediate effect and until further notice, suspend the leaver process in respect of the individuals listed, including: deletion or expiry of mailboxes, OneDrive/Drive stores and chat identities; licence removal that triggers data deletion; and wiping, reissue, repair or disposal of any device they used. For individuals who have already left, state per person what survives today, in which systems, and what was deleted or reissued, with dates. Confirm each step in writing with effective date and time."

B · NOTICE TO A FORMER EMPLOYEE (para 4.2-style)

"We act for [client] in [dispute]. Documents and communications from your employment, including any work-related material on personal devices or accounts, may be relevant and must not be deleted, altered or disposed of. Please: (1) confirm you will preserve such material; (2) tell us what work-related material you hold and where; and (3) contact [name] to arrange collection of work-related material under a protocol that protects your personal information. This is a preservation request required by court rules, not an accusation."

C · TIERED COUNTER-OFFER ON CUSTODIANS (to the opponent)

"Of the six additional custodians you propose, our register records the following: [names, roles, issue-connection, per-custodian volumes]. Sampling of their traffic deduplicated against our reviewed custodians shows unique-document yield of [x]%. We are not prepared to add them to full review. We offer: (1) collection and processing (not review) of [names], with the data held; and (2) promotion to review if [trigger: sampled richness above x% / identified gaps in productions]. This offer holds the position at proportionate cost while preserving every option; if it is not acceptable, we propose the point be listed for Disclosure Guidance."

D · PERSONAL-DEVICE PROTOCOL (to a custodian, with client HR)

"To meet the parties' disclosure duties, work-related material on your personal [phone/accounts] must be preserved and, to the defined extent, collected. The process: an independent examiner will extract only the categories listed in the Schedule [apps, counterparties, date ranges]; personal material outside the Schedule will be screened out by the examiner and not provided to the legal team; you may have a representative present; the extraction will be documented and your device returned the same day. Please confirm a convenient date within [7] days."

SECTION 25

Checklist: custodian selection essentials

- ☐ Events mapped per issue; candidates extracted from events, not the org chart
 - ☐ Forgotten classes deliberately checked: deputies, assistants, finance, technical, complaint-handlers, leavers, contractors
 - ☐ Non-custodial half built: shared mailboxes, repositories, systems – each with a steward
 - ☐ Leaver freeze issued day one; per-leaver survival verified in consoles
 - ☐ Tier 1 candidates interviewed with the 40-question bank; verified/assumed marked
 - ☐ Personal-channel exposure asked of every custodian; *Phones 4U* route planned where it exists
 - ☐ Three tiers assigned with per-custodian volumes and costs
 - ☐ Preservation executed by risk, not tier; dates recorded
 - ☐ Custodian defects (gaps, wiped devices) scheduled with dates, recovery paths and disclosure route
 - ☐ EDA communication analysis run; list re-ranked on data
 - ☐ Declines recorded with reasons in the register
 - ☐ Register two-layered (exhibitible / privileged) with named owner and change log
 - ☐ DRD Section 2 schedule generated from the register and reconciled against its change log
 - ☐ Tiered offers prepared for the custodian negotiation, with numbers
 - ☐ Register review diarised at each phase gate through productions
-

SECTION 26

Red flags

IN YOUR OWN EXERCISE

- The list was settled in a meeting with no interviews and no minutes.
- Every custodian is a manager; no author of the operative documents is on it.
- A name appears constantly in the documents' cc lines but not on the register.
- A key custodian's interview answers conflict with the console evidence (folders, delegates, devices).
- "We don't use WhatsApp for work" from a team whose counterparty's letter quotes a WhatsApp message.
- Leavers' survival status is assumed from policy rather than verified per person.
- The register and the DRD schedule disagree, and nobody can say why.

IN THE OPPONENT'S LIST

- The obvious actor in the pleaded events is missing without explanation.
- All custodians are senior; the drafters and doers are absent.
- Former employees involved in the events are omitted, or their data declared unavailable without dates or specifics.
- No shared mailboxes or systems despite a business that plainly runs on them.
- Date ranges that conveniently end just before the interesting period.
- Refusal to state selection criteria or provide per-custodian volumes.
- A defect (gap, wipe, deletion) emerging late that their early correspondence never mentioned.

SECTION 27

When to involve a digital forensic expert

- **The hot custodian.** Where an individual's conduct is in issue (departure, exfiltration, deletion), their devices and accounts need forensic sequencing – image before confrontation, artefacts before interviews (the Marsh pattern), with method statements for the record.
- **Defect documentation.** Gaps and wipes need expert characterisation: what exactly is missing, what the platform's logs say about when and how, and which recovery paths (backups, counterpart copies, artefacts) remain. An expert-documented defect reads as diligence; a lawyer-described one reads as hope.
- **Attribution doubts.** Shared logins, delegate access and "that wasn't me" defences turn custodian data into an attribution problem – authentication logs, device artefacts and stylometry territory.
- **Personal-device collection.** The privacy-screened, examiner-mediated extraction that makes *Phones 4U* requests workable is an examiner's product; it converts refusal-prone demands into accepted protocols.
- **Leaver machines in the cupboard.** Before anyone "has a quick look" at a returned device, forensic triage decides whether it needs imaging – the quick look is how artefact evidence dies.

SECTION 28

How the rules differ: Scotland, NI, arbitration, tribunals, criminal

Forum	Custodian position
England & Wales, non-B&PC	CPR 31.7's reasonable-search factors and PD 31B's questionnaire assume custodian identification; <i>Digicel</i> and <i>Phones 4U</i> both arose under Part 31 and apply directly.
Scotland	Recovery by specification: no custodian lists as such, but drafting effective specifications requires knowing whose records the havers hold; preservation practice mirrors the register defensively.
Northern Ireland	Order 24 discovery: the affidavit of documents obliges the deponent to have made proper inquiry – functionally, a custodian exercise the deponent must be able to describe.
Arbitration	IBA Rules Art 3 requests are drafted per custodian in practice ("documents of Mr X concerning..."); tribunals weigh burden objections on custodian counts, and your shadow register of the opponent's people drafts better requests.
Employment tribunals	Disclosure by order; the respondent's custodian choices (line manager, HR, the decision-makers) are routinely tested, and personal-channel evidence (messages between managers) features heavily in dismissal and discrimination claims.
Criminal proceedings	CPIA reasonable lines of enquiry translate to whose devices and accounts investigators must consider – suspects, complainants (with the CPS's proportionality constraints on complainant phones), and third parties; the AG's Guidelines (2024) govern digital scoping, and FSR Code requirements attach to extraction and examination.

SECTION 29

Glossary

BYOD	Bring your own device: business data on personal hardware.
Change log	The register's record of every addition, demotion, promotion and decline, with dates and reasons.
Communication analysis	Analytics over senders/recipients/frequency used to validate or re-rank the custodian list.
Custodian	Person whose document and communication bundle is preserved and potentially collected.
Custodian bundle	The full source set following a person: mailbox, cloud store, devices, chat identity, personal-channel exposure.
Defect schedule	Per-custodian record of known gaps, wipes and losses, with dates and recovery paths.
Delegate access	Authority to operate inside another person's mailbox, diary or files.
EDA	Early data assessment: pre-review measurement of volumes, duplication and communication patterns (Guide 8).
Non-custodial source	Organisational data owned by no individual: shared mailboxes, repositories, systems, logs.
Register	The custodian and source register: the versioned master document this guide builds.
Steward	The named person answerable for a non-custodial source.
Tiering	Grading custodians into review / hold / monitor classes with promotion triggers.

SECTION 30

Authoritative UK references

- PD 57AD (preservation paras 3.1-4.4 incl. former employees; DRD custodian questions) and the Disclosure Review Document: [justice.gov.uk – PD 57AD](https://www.justice.gov.uk/pd-57ad); [DRD form](#)
- CPR 31.7 (reasonable search) and PD 31B: [justice.gov.uk – CPR 31](https://www.justice.gov.uk/cpr-31)
- *Phones 4U Ltd v EE Ltd* [2021] EWCA Civ 116 (personal devices and accounts): caselaw.nationalarchives.gov.uk
- *Digicel (St Lucia) Ltd v Cable & Wireless plc* [2008] EWHC 2522 (Ch): [bailii.org](https://www.bailii.org/)
- *McParland v Whitehead* [2020] EWHC 298 (Ch) (Issues for Disclosure driving scope): caselaw.nationalarchives.gov.uk
- ICO: employment practices and monitoring-at-work guidance; UK GDPR resources: ico.org.uk; UK GDPR / DPA 2018 / Data (Use and Access) Act 2025: legislation.gov.uk
- Law Society practice notes on disclosure; SRA Standards and Regulations (competence and supervision duties bearing on disclosure conduct): lawsociety.org.uk; sra.org.uk
- Attorney General's Guidelines on Disclosure (2024): gov.uk; CPS guidance on digital material incl. complainant devices: cps.gov.uk
- Forensic Science Regulator statutory Code (v2, October 2025): gov.uk/fsr

SECTION 31

How a specialist laboratory can assist

Custodian work sits exactly where legal judgement meets technical verification, and a specialist electronic disclosure and digital forensics laboratory earns its place at four moments:

- **Building the register:** technical attendance at interviews, console verification of every stated bundle, per-custodian volume and cost estimates that make tiering an arithmetic exercise.
- **Preserving the risky rows:** same-day leaver freezes verified per platform, device quarantine and imaging (before confrontation where conduct is in issue), and defect schedules that document gaps as evidence rather than admissions.
- **Validating the list:** communication analysis across collected sources, dedupe-based uniqueness testing of marginal names, and the sampling that turns tier disputes into numbers.
- **Reaching the difficult bundles:** privacy-screened personal-device extraction under *Phones 4U*-compliant protocols, shared-mailbox and delegate-access collection that preserves attribution, and cross-border custodian handling with local-law awareness.

NPCC-aligned handling, ISO 17025 aligned practice, and examiners who can stand behind every register row they touched. Instruct early: the custodian decisions taken in week one are the ones the whole case pays for – or profits from.



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



SCAN TO CONTACT

e-discovery.uk / +44 (0)20
7164 6971