



Finding the Evidence: A Lawyer's Map of Modern Electronic Data Sources

Computers, phones, email, cloud platforms, Teams, Slack, file servers, NAS, SaaS, databases, CCTV, backups, CRM, ERP, social media, messaging apps, logs, IoT and third parties – where evidence lives today, how volatile each source is, and how to map a client's estate before anything disappears.

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

You cannot preserve, search or disclose what you have not found. This guide maps the modern electronic evidence estate – eight families of sources, their volatility, and the questions that surface them – and provides the questionnaire and workflow for building a defensible data map at the start of any matter.

1	Executive summary	3
2	The problem in plain English: the evidence map has exploded	4
3	Why it matters legally: search duties start with source identification	5
4	Important terminology	6
5	The evidence-source map: eight families	7
6	Family 1: endpoint devices – computers, phones, tablets, removable media	8
7	Family 2: email systems – corporate, hosted, webmail and personal	9
8	Family 3: cloud productivity and collaboration – M365, Google, Teams, Slack	10
9	Family 4: file storage – servers, NAS, sync-and-share platforms	11
10	Family 5: structured systems – databases, accounting, CRM, ERP	12
11	Family 6: messaging and social – WhatsApp, Signal, SMS, social media	13
12	Family 7: logs and the physical world – CCTV, access control, IoT, web logs	14
13	Family 8: backups, archives and third-party holders	15
14	Volatility: which sources die first	16
15	The source-mapping workflow: seven steps to a defensible data map	17
16	Decision tree: which sources to pursue, park or release	18
17	Worked example 1: mapping Aldgate's estate in a fortnight	19
18	Worked example 2: the opponent's estate – Harlow, its MSP and the backup vault	20
19	Worked example 3: one custodian, eleven sources – the departed director	21
20	The custodian and source questionnaire: 43 questions in three parts	22
21	Preservation and collection notes by family	24
22	Privilege and confidentiality considerations	25
23	UK GDPR and data minimisation when mapping sources	26
24	Proportionality: mapping everything, collecting selectively	27
25	Common mistakes and how to avoid them	28
26	Technical limitations lawyers should understand	29
27	Questions lawyers should ask the opponent about their sources	30
28	Questions lawyers should ask a forensic or eDisclosure provider	31
29	Suggested wording for instructions	32
30	Checklist: the source-mapping essentials	33
31	Red flags	34
32	When to involve a digital forensic expert	35
33	How the rules differ: Scotland, NI, arbitration, tribunals, criminal	36
34	Glossary	37
35	Authoritative UK references	38
36	How a specialist laboratory can assist	39

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

Every disclosure failure begins the same way: a source nobody thought to ask about. The mailbox was preserved but the Teams channels were not; the laptop was imaged but the NAS under the stairs was reformatted; the CRM held the real negotiation history while everyone argued about email. Modern organisations scatter evidence across dozens of systems, most of them invisible to the lawyers until an IT manager mentions one in passing – often after its retention clock has run out.

This guide is the map. It organises the modern estate into **eight families**: endpoint devices; email; cloud productivity and collaboration; file storage; structured systems; messaging and social; logs and the physical world; and backups, archives and third parties. For each family it explains what evidence lives there, what is commonly missed, how volatile it is, and what to do in the first week. It then provides the working tools: a volatility ranking that tells you what dies first; a seven-step workflow for building a data map; a decision tree for pursuing, parking or releasing each source; a 43-question custodian and source questionnaire; and question banks for the opponent and your provider.

Two principles run through everything. First, **map everything, collect selectively**: identification costs almost nothing and forecloses nothing, while a source you never identified cannot be preserved, negotiated over, or defended at a CMC. Second, **volatility sets the order of work**: CCTV overwrites in days, audit logs in months, backups on rolling schedules – the map must be built in the order the evidence is dying, not in the order the org chart suggests.

THE GUIDE IN ONE PARAGRAPH

In week one, interview IT and the key custodians with the Section 20 questionnaire, sketch the estate against the eight families, and rank every source by volatility. Preserve the dying sources first, whatever their apparent importance. Sign the data map off with the client's IT lead, date it, and treat it as a living document. Everything downstream – custodians (Guide 5), control (Guide 6), reasonable search (Guide 7), the DRD (Guide 15) – stands on this map.

SECTION 2

The problem in plain English: the evidence map has exploded

Twenty years ago a company's documents lived in three places: filing cabinets, a file server and an email server. A competent IT manager could describe the whole estate in an afternoon. Today the same mid-sized business runs Microsoft 365 or Google Workspace; laptops and phones that sync some things and silo others; Teams or Slack carrying the conversations that used to be email; a dozen SaaS platforms (CRM, HR, finance, design, support-ticketing) each holding its own records under its own retention rules; personal devices under BYOD policies; WhatsApp groups that "aren't official but everyone uses"; cloud backups run by an outsourced MSP; and a decommissioned server "somewhere in storage".

Three features of this landscape catch lawyers out:

- **Nobody sees the whole estate.** IT knows the systems it administers but not the shadow IT the sales team adopted; custodians know their own habits but not the infrastructure; the MSP knows the backups but is never in the room. The map exists only when someone assembles it.
- **Sources are not where the data is.** A "document on a laptop" may really live in OneDrive, cached locally, with versions in SharePoint, copies in email attachments, references in Teams, and a backup at the MSP. Guide 44 onwards in this series treats this as a formal discipline – every device has associated evidence locations – but the instinct starts here: always ask where else the same evidence lives.
- **Every source has its own clock.** Retention policies, rolling backups, licence-driven deletion of leavers' accounts and CCTV overwrite cycles all run regardless of your litigation. The map is a race against defaults.

THE QUESTION THAT BUILDS THE MAP

The single most productive question in any scoping interview is not "what systems do you have?" but "**show me how a document is born, lives and dies here** – who creates it, in what tool, where it goes when shared, and what happens when someone leaves." Systems lists produce inventory; lifecycle stories produce evidence paths.

SECTION 3

Why it matters legally: search duties start with source identification

Source identification is not a technical nicety; it is where the legal duties bite first.

- **Preservation.** PD 57AD paragraph 3.1 requires a party to take reasonable steps to preserve documents in its control that may be relevant, once proceedings are contemplated – and paragraph 4 spells out suspension of deletion processes and notification of employees and former employees. You cannot suspend a deletion process on a system you have not identified. The duty is judged with hindsight: "we did not know we had it" rarely survives an audit log showing IT did.
- **The DRD and Section 2.** The Disclosure Review Document requires each party to describe where its documents are held, including systems, custodians and third parties. A data map is simply DRD Section 2 done properly and early; Guide 15 shows the form consuming the map's outputs.
- **Reasonable search.** Under paragraph 6.4 and the Model D/E duties, and under CPR 31.7 elsewhere, the reasonableness of a search is assessed source by source. *Digicel (St Lucia) Ltd v Cable & Wireless plc* [2008] EWHC 2522 (Ch) remains the touchstone: parties who unilaterally excluded sources (there, backup tapes and additional custodians) had the decision remade by the court. Identification first, exclusion by agreement or order after.
- **Known adverse documents.** The paragraph 3.1(2) duty to disclose known adverse documents (Guide 16) extends to knowing where such documents would live; unusual repositories – the personal Gmail forwards in the series example – are found by mapping, not by luck.
- **Costs and sanctions.** Late-discovered sources reopen collections, redo searches and postpone trials, and the party responsible pays: the adverse costs and inference machinery (paras 10.3, 17-18; CPR 3.1 generally) treats "we found another server" very differently depending on whether the map shows diligence or drift.

THE CAUTIONARY CLASSIC

Earles v Barclays Bank plc [2009] EWHC 2500 (QB) docked a winning party's costs for failing to preserve and produce electronic records it plainly held; *Digicel* shows scope being retrofitted by the court when sources were excluded unilaterally. Both predate PD 57AD; the modern regime has only raised the price of an incomplete map.

SECTION 4

Important terminology

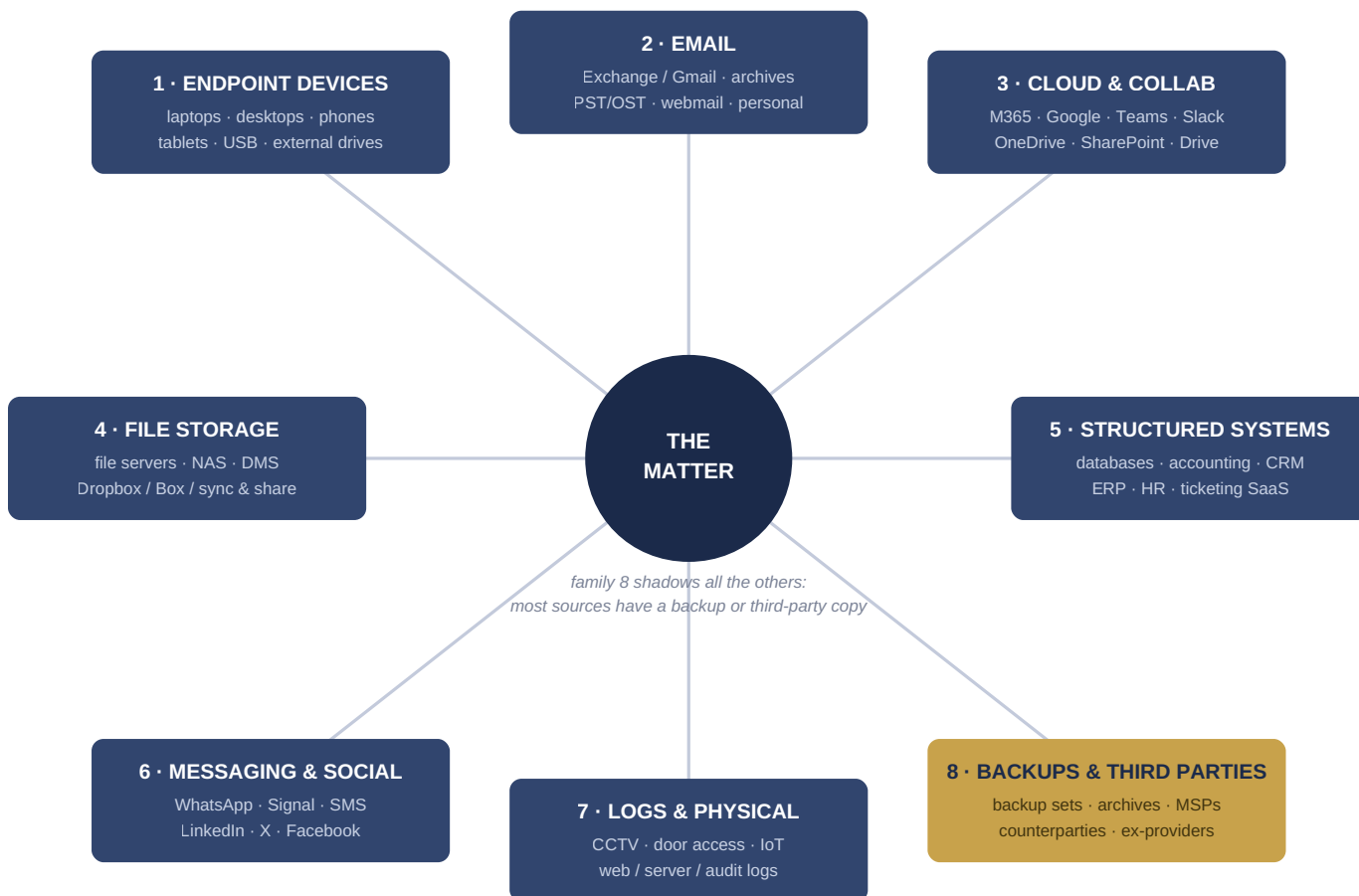
Term	Meaning in the source-mapping context
Data map	The dated, signed-off inventory of an organisation's evidence sources: system, owner, location, contents, retention, volatility, preservation status.
Custodian	A person whose documents and communications are collected; custodial sources follow people (mailbox, laptop, phone). Guide 5 covers selection.
Non-custodial source	A source that belongs to the organisation rather than a person: shared mailboxes, file shares, databases, SaaS platforms, logs.
Shadow IT	Systems adopted by teams without IT governance – personal Dropbox, WhatsApp groups, a free Trello board. Invisible on official inventories; found by asking custodians how work actually gets done.
MSP	Managed service provider: an outsourced IT operator who often controls backups, email hosting and admin consoles – a third party holding your client's evidence.
SaaS	Software as a service: applications hosted by vendors (Salesforce, Xero, HubSpot). Data lives in the vendor's cloud under contract terms that govern export and retention.
Retention policy	Automated rules deleting or archiving data after set periods; the default clocks the preservation duty must stop (Guide 25 covers the collision in depth).
Volatility	How quickly a source's evidence disappears by default: overwrite cycles, rolling windows, licence deletion. Section 14's ranking drives work order.
BYOD	Bring your own device: business data on personal phones and computers, raising mixed control, privacy and collection questions (Guide 68 to come).
Audit log	System-generated records of user and administrator actions (logins, deletions, downloads, sharing). Often the evidence about the evidence, with short default retention.

SECTION 5

The evidence-source map: eight families

Figure 1 is the map this guide is named for. Everything an organisation holds falls into one of eight families around the matter at the centre; Sections 6 to 13 tour them in turn. The map's use is diagnostic: in any scoping interview, tick the families as they are covered, and treat any family with no entries as a question, not an answer – almost no modern business genuinely has "no structured systems" or "no logs".

Figure 1 · The evidence-source map: eight families around every matter



Gold marks the family lawyers most often forget: the copies. When a primary source is gone, damaged, encrypted or denied, family 8 is where the alternative evidence path usually runs.

SECTION 6

Family 1: endpoint devices – computers, phones, tablets, removable media

What lives there. Local documents and downloads; email caches (OST files); chat app databases; browser history; recent-file and USB-connection artefacts; deleted-but-recoverable material; and on phones, the richest single evidence source in modern practice: messages, photos with location data, call logs, app data (Guide 61 will go deep).

Commonly missed. The previous laptop (many businesses reissue rather than wipe... eventually); personal devices doing business work under BYOD; tablets; USB drives and external disks (Guides 47-48); the pool of returned leaver devices in a cupboard, unwiped and unindexed.

Volatility. Medium as to files, high as to artefacts: reissuing a leaver's laptop destroys the artefact record even if files were copied off first; phones are wiped on upgrade cycles; MDM policies can remote-wipe (Guide 26). The series example turns partly on exactly this: **James Marsh's Aldgate phone was wiped and reissued on his departure** in March 2025, closing one source – while his **laptop was quarantined and imaged before anyone confronted him**, preserving USB and upload artefacts that later mattered.

First-week moves. Freeze reissue/wipe cycles for named custodians; quarantine leaver devices; record asset registers; for any device where user actions may be in issue, forensic imaging before continued use (Guides 31-33).

SECTION 7

Family 2: email systems – corporate, hosted, webmail and personal

What lives there. The chronological backbone of most disputes: messages, attachments, calendar entries, and the metadata (headers, routing, read status) that dates and attributes them. Modern corporate email means Exchange Online or Gmail, with litigation-hold, archive and recoverable-items machinery (Guides 23, 53, 58).

Commonly missed. Shared and role mailboxes (the series' *contracts@* mailbox held negotiations no individual custodian's mailbox showed); leavers' mailboxes deleted 30 days after licence removal; local PST archives on laptops and file shares; auto-expiring retention labels; and business mail diverted to **personal accounts** – the 40 forwards to a personal Gmail account that Guide 16's certificate exercise surfaced were found because an interviewer asked, and were adverse-document territory, not just a mapping footnote (Guide 69 to come).

Volatility. Low while accounts live, cliff-edged when they end: the leaver-account deletion clock is among the most dangerous defaults in the estate.

First-week moves. Litigation hold on named mailboxes including shared ones; stop leaver-account deletion for anyone connected to the issues; sweep laptops and shares for PSTs; ask every key custodian, in terms, about personal-account use for business.

SECTION 8

Family 3: cloud productivity and collaboration – M365, Google, Teams, Slack

What lives there. Increasingly, the working life of the business: OneDrive and Google Drive personal stores; SharePoint sites and Shared Drives; Teams and Slack messages, channels, meeting recordings and wiki pages; version histories that show a document's evolution; sharing records showing who could see what, when; and the platform **audit logs** recording access, downloads, deletions and admin actions (Guide 57).

Commonly missed. Private channels and DMs (licensed and retained differently from public channels); meeting recordings and transcripts; the audit log's own retention limit – on many licences the default window is measured in months, and the evidence about deletions expires quietly. In the series example, Aldgate's E5 tenancy held 12 months of Purview audit data: the **February 2025 bulk-deletion entries were exported on 26 January 2026**, days after the first scoping meeting, precisely because the map flagged the log's rolling window.

Volatility. Retention-policy-driven for content (Teams chat policies can be short); rolling and unforgiving for audit logs. Version histories thin out over time on some plans.

First-week moves. Identify tenancy, licences and retention policies; suspend deletion policies for relevant scopes (the series hold, completed 4 February 2026, included suspending a 12-month Teams retention policy); export the audit log for the relevant period *now*, not when it becomes an issue.

SECTION 9

Family 4: file storage – servers, NAS, sync-and-share platforms

What lives there. Departmental shares with decades of sediment; project folders; the design office's CAD vault; document management systems with version and access histories (Guide 75); NAS boxes serving small offices (Guide 44); Dropbox/Box/Egnyte estates that predate or bypass the corporate cloud.

Commonly missed. Access permissions and access logs (who *could* reach the folder is often as probative as what it contains – the series' Issue 3 Model C request was for the "**R&D/CAD-Masters**" and "**R&D/CAD-Archive**" access logs, **November 2024 to March 2025, in native CSV**); snapshots and shadow copies holding historical states (Guide 50); orphaned shares from departed teams; the decommissioned server in storage.

Volatility. Content low; logs and snapshots medium-to-high (rolling windows, snapshot pruning); decommissioned hardware high in a different way – disposal runs on asset-management schedules nobody connects to litigation.

First-week moves. Inventory shares against the org chart; capture permission listings and available access logs for hot folders; locate snapshots and their retention; put a hold notice on hardware disposal.

SECTION 10

Family 5: structured systems – databases, accounting, CRM, ERP

What lives there. The records businesses actually run on: transactions, ledgers, orders, deliveries, customer interactions, support tickets, HR files. Unlike documents, this evidence is **records in tables**: the "document" often has to be generated by a query, and the probative payload includes amendment histories, user stamps and approval workflows (Guides 71-74).

Commonly missed. That exporting a spreadsheet is not the same as preserving the database (relationships and audit trails are lost); change logs proving when a record was altered; archived or legacy systems from before a migration ("the old Sage is on the retired server"); SaaS platforms' own audit trails and their contractual export limits.

Volatility. Core records low; audit and change logs often on short rolling windows; legacy systems vulnerable to decommissioning; SaaS data vulnerable to subscription lapse – when the contract ends, the vendor's deletion clock starts.

First-week moves. List every line-of-business system touching the issues; establish each one's audit-trail retention; stop decommissioning; for SaaS, check the contract's data-return terms and renewal dates before they check you.

SECTION 11

Family 6: messaging and social – WhatsApp, Signal, SMS, social media

What lives there. The candid record. Formal positions live in email; what people actually thought lives in WhatsApp. Messages, voice notes, images, group-chat dynamics (who was in the group, when they joined and left), and on social platforms, posts, DMs and connection histories (Guides 63-67).

Commonly missed. Disappearing-message settings silently destroying evidence prospectively (a hold must address them: Harlow's scoping in the series example included **turning off WhatsApp disappearing messages and documenting the change**); backups of message databases in iCloud/Google that outlive the handset; the fact that each participant's device is an independent copy – the counterpart's phone is an alternative evidence path when your custodian deleted the thread; platform ephemerality by design (Signal; Guide 64).

Volatility. High. Settings, handset loss, app reinstalls and upgrade cycles all destroy; group membership changes rewrite what a new collection can see.

First-week moves. Ask every custodian which apps carry business traffic (expect understatement; ask for examples, not policy answers); disable ephemerality and document it; preserve devices before handset upgrades; identify which counterparties hold the same threads.

SECTION 12

Family 7: logs and the physical world – CCTV, access control, IoT, web logs

What lives there. Corroboration and chronology: CCTV and DVR/NVR systems (Guide 77); door-access and swipe-card logs (Guide 78); web, application and authentication logs with IPs and timestamps (Guide 79); vehicle trackers, printers, VoIP call records, and the expanding IoT fringe. Rarely the main event; frequently the tie-breaker – the log that proves who was in the building, logged in, or downloading at the disputed moment.

Commonly missed. All of it, until too late: these systems belong to facilities and security teams no litigation hold reaches by default, and their retention is the shortest in the estate.

Volatility. The highest in the map. CCTV commonly overwrites in 14-31 days; access-control systems and VoIP platforms keep weeks to months; authentication logs rotate on size limits that can mean days.

First-week moves. If any issue involves *who did what, when, where*: same-day preservation requests to facilities/security; export (do not just "retain") CCTV covering key dates using the system's native export (Guide 77 explains why screen recordings disappoint); pull authentication and VPN logs for the window before they rotate.

SECTION 13

Family 8: backups, archives and third-party holders

What lives there. Copies of nearly everything else, at points in time: backup sets on rotation (the series' Aldgate ran **Veeam on a 30-day rolling cycle plus monthly snapshots kept 12 months**); long-term archives; journaling systems capturing every email; and the third parties – MSPs, former IT providers, hosting companies, counterparties, professional advisers – who hold your client's data under their own arrangements. Harlow's estate in the series example includes the decisive instance: an **MSP holding a 7-year backup vault**, reachable through a contractual inspection right (clause 14), which Guide 6 analysed as a control question and Section 18 below revisits as mapping.

Commonly missed. That backup *expiry* is deletion on a schedule (a hold that does not pause rotation destroys historical states weekly); that "we back up nightly" tells you nothing about what is *restorable*; former providers still holding data after contract end; and the map's mirror image – what counterparties and opponents hold that duplicates what your client lost (the alternative-evidence-path habit).

Volatility. Structurally scheduled: every rotation is a small deletion event. Proportionality governs whether backups are searched (Guide 49), but identification and a rotation decision are week-one, always.

First-week moves. Get the backup schedule in writing (what, how often, kept how long, restorable how); decide explicitly – and record – whether to pause rotation or preserve specific sets; write to third-party holders (Guide 29's preservation-notice practice); list contracts giving rights over third-party-held data.

SECTION 14

Volatility: which sources die first

Figure 2 ranks the families by how quickly their evidence disappears under default settings. It is the work-ordering tool: preservation effort flows top-down, whatever the apparent importance of the sources, because importance can be argued later but overwritten CCTV cannot.

Figure 2 · The volatility ladder: default lifetimes, and what kills each source

DAYS TO WEEKS – ACT SAME-DAY

CCTV / DVR overwrite (often 14-31 days) · rotating auth/VPN logs · disappearing-message settings · volatile device state

WEEKS TO MONTHS – ACT IN WEEK ONE

backup rotation cycles (e.g. 30-day rolling) · leaver-account deletion clocks · short Teams/Slack retention policies · access-control logs

MONTHS – ACT BEFORE THE WINDOW CLOSES

platform audit logs (e.g. 12 months on M365 E5, less on lower licences) · monthly backup snapshots · SaaS audit trails · version histories

QUARTERS TO YEARS – SCHEDULED THREATS

retention-policy deletions · device reissue and upgrade cycles · system migrations and decommissioning · SaaS contract expiry

STABLE UNTIL TOUCHED

live mailboxes and files under hold · archives and journals · quarantined devices · forensic images · papers in storage

THE RULE: PRESERVE IN VOLATILITY ORDER, ARGUE IN IMPORTANCE ORDER

A source's place on this ladder, not its likely evidential weight, sets when you deal with it. Cheap preservation now keeps every argument available later.

Every default is a deletion schedule. The map is not finished until each source carries a volatility rating and a dated preservation decision.

SECTION 15

The source-mapping workflow: seven steps to a defensible data map

#	Step	How	Output
1	Frame the issues	From the pleadings or dispute correspondence, list what has to be proved or rebutted; the map is issue-led, not inventory-led	Issue list (feeds Guide 13 later)
2	Interview IT and the MSP	Systems inventory, tenancy and licences, retention policies, backup schedule, leaver process, admin consoles; use questionnaire Part A	Infrastructure schedule
3	Interview key custodians	How work is actually done: apps, devices, personal accounts, shadow IT; use questionnaire Part B; expect the official and real answers to differ	Custodian source profiles
4	Sweep for the forgotten	Leaver devices, legacy systems, storage rooms, former providers, counterparty copies; use questionnaire Part C	Additions to the map
5	Rate volatility and preserve	Ladder every source (Figure 2); execute same-day and week-one preservation; record each decision with dates	Preservation log (feeds the hold: Guide 22)
6	Sign off the map	One document: source, family, owner, contents, retention, volatility, preservation status, collection stance; client IT lead signs and dates it	The data map v1
7	Maintain it	New custodians, new systems, corrections from later interviews; version the map; it becomes DRD Section 2 and the CMC narrative	Living map + change log

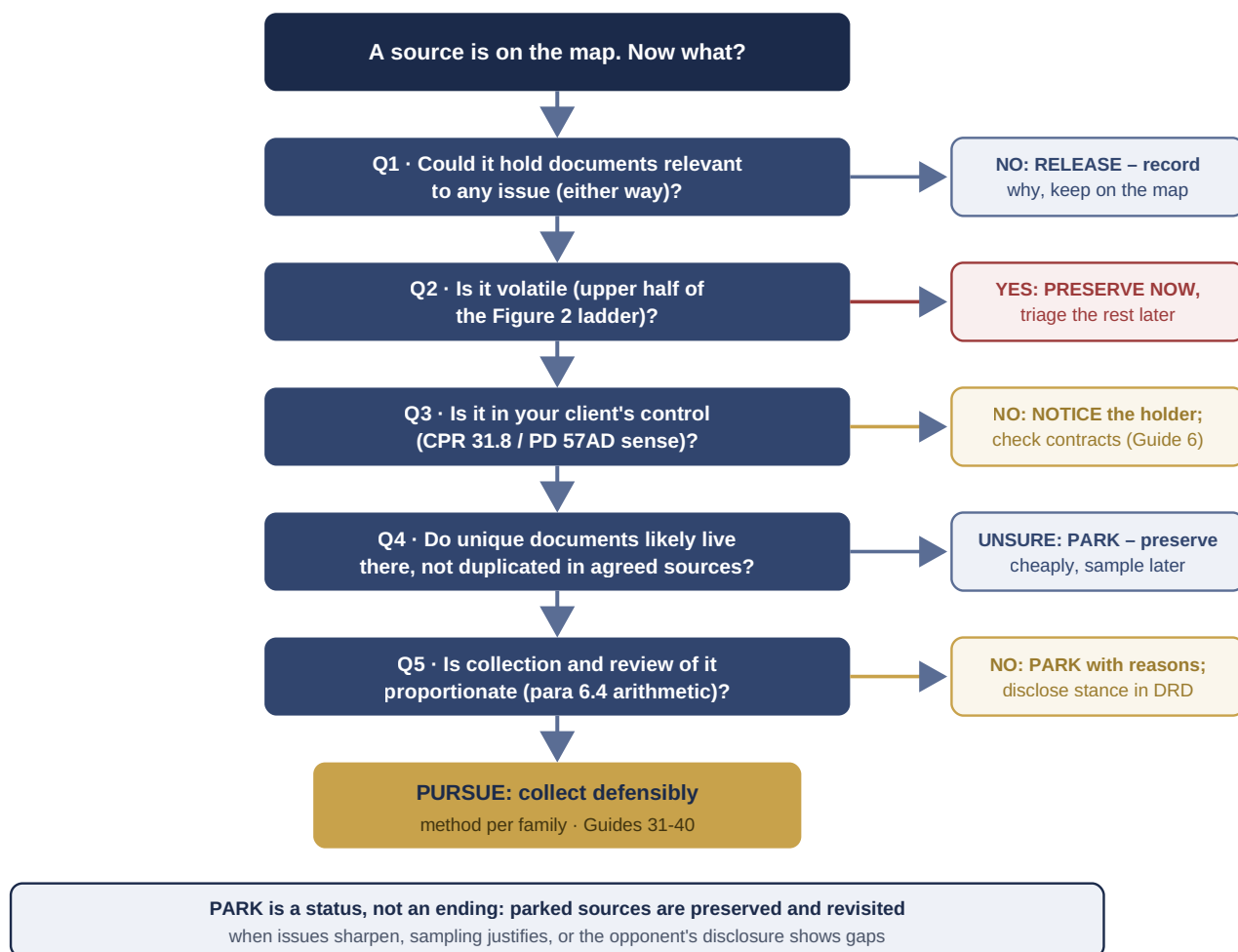
In the series example this workflow ran from the first Aldgate meeting on **Friday 23 January 2026** to a data map **signed off by the IT manager on 30 January 2026** – a week, for a business of Aldgate's size, with the audit-log export (26 January) and the completed hold (4 February) falling out of steps 5 and 6. Speed came from doing steps 2 and 3 in parallel, not sequence.

SECTION 16

Decision tree: which sources to pursue, park or release

Identification is cheap; collection and review are not. Figure 3 is the triage each mapped source goes through – and revisits as the case develops.

Figure 3 · Source triage: every mapped source gets a dated decision



Release decisions belong on the map too: the CMC question is never only "what did you search?" but "what did you decide not to search, and why?" A dated, reasoned release is defensible; an absence is not.

SECTION 17

Worked example 1: mapping Aldgate's estate in a fortnight

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

Aldgate, a components manufacturer, suspects its former commercial director James Marsh (left 21 March 2025, joined competitor Harlow) misused confidential pricing and took CAD files, and disputes Harlow's termination of their supply agreement. The GC sent a "keep everything" email on 15 January 2026; solicitors first met the client on Friday 23 January 2026.

Day 1 (23 Jan). Scoping meeting runs the Section 20 questionnaire. The eight-family sweep immediately surfaces: M365 E5 tenancy (Exchange, OneDrive, SharePoint, Teams); a CAD vault on-premises; Veeam backups (30-day rolling, monthly snapshots kept 12 months); the *contracts@* shared mailbox; sales team WhatsApp habits; and two ticking clocks – Purview audit retention of 12 months, and Marsh's departure ten months earlier.

Day 2-4. Volatility triage (Figure 2): the audit window covering Marsh's final months was months from expiry, so the **Purview export of the February 2025 deletion entries happened on 26 January** – before custodian interviews, before strategy, before anything slower. Marsh's asset-register entries answered the device questions: phone wiped and reissued on departure (source closed; noted with dates for later explanation), laptop quarantined and imaged (source preserved).

Day 5-8. IT interview completes the infrastructure schedule; custodian interviews (Okafor, Devlin, Szabo) profile the human sources – Szabo's interview fixes the CAD folder structure and its access-log capability, which becomes Issue 3's Model C request a year later. The hold (Guide 22's machinery) completes on **4 February**, including suspension of the 12-month Teams retention policy.

Day 8. The data map v1 – 23 sources, family-classified, volatility-rated, preservation status per source – is **signed off by Aldgate's IT manager on 30 January 2026**. It is versioned thereafter and becomes, nearly verbatim, DRD Section 2 in November (Guide 15).

WHAT MADE IT DEFENSIBLE

Not completeness – v1 missed things (the personal-Gmail forwarding surfaced only at the Guide 16 certificate interviews). What made it defensible: dated decisions, volatility-first ordering, honest recording of closed sources (the wiped phone), and a signed, versioned document showing the exercise was systematic. Maps are judged by their method, not their omniscience.

SECTION 18

Worked example 2: the opponent's estate – Harlow, its MSP and the backup vault

You map the opponent's estate too – from the outside, then through the DRD. Aldgate's team built a "shadow map" of Harlow from: the industry's standard toolchain; email headers and document metadata in pre-action correspondence; Companies House and job-advert clues about systems ("experience of SolidWorks PDM an advantage"); and Marsh's own knowledge of what he took where.

The shadow map's biggest hit was inferential: a business of Harlow's profile would outsource IT, and outsourced IT means an MSP holding backups. The pre-action preservation letter (Guide 29 practice) therefore asked expressly about third-party-held backups and their rotation. Harlow's answer disclosed the **MSP with a 7-year backup vault**; the supply agreement's **clause 14 inspection right** gave a contractual route to it, and Guide 6 analysed the control consequences. At the Harlow scoping meeting in late February 2026, its own solicitors – to their credit – instructed the MSP the same day, before rotation ate further months.

THE MIRROR-MAP HABIT

For every source your client lost, ask which external holder has a copy: the counterparty's inbox holds the emails your client deleted; the MSP's vault holds the file server's history; the departed employee's new employer holds the devices he filled. Family 8 thinking, pointed outward, is how gaps become requests instead of apologies.

SECTION 19

Worked example 3: one custodian, eleven sources – the departed director

Mapping is most concentrated around a single hot custodian. For Marsh, the source list ran to eleven entries across six families:

Source	Family	Status at mapping (Jan 2026)	Outcome
Aldgate mailbox	2	Preserved; but a Nov 2024-Mar 2025 gap in sent items	Gap disclosed (DRD Q8 entry, Guide 15); alternatives pursued
Aldgate laptop image	1	Quarantined and imaged before confrontation	USB and upload artefacts available
Aldgate phone	1	Wiped and reissued on departure	Closed; fact and dates recorded
OneDrive + SharePoint activity	3	Under hold; versions intact	Collected per protocol
Purview audit log	3/7	12-month rolling window	Feb 2025 deletion entries exported 26 Jan 2026
CAD vault access logs	4/7	Retained; export format confirmed with Szabo	Issue 3 Model C class (native CSV, Nov 2024-Mar 2025)
Veeam monthly snapshots	8	12 months back = covers final employment months	Rotation paused for relevant sets
Personal Gmail	2	Suspected only	40 forwards confirmed at certificate-stage interviews (Guide 16)
Personal WhatsApp	6	Outside control; counterpart devices exist	Kept hypothetical; preservation raised with Harlow
Marsh's Harlow mailbox	2	Opponent-controlled	Held for CMC; targeted Model C class ordered (Guide 15)
Marsh's Harlow devices	1	Opponent-controlled; Harlow onboarded him with independent forensics	Preservation confirmed inter-partes

The table demonstrates the method: **every closed source generated an alternative path** (wiped phone → audit logs, counterpart devices, snapshots; mailbox gap → recipients' copies, backup restores), and every opponent-held source generated a request rather than a hope.

SECTION 20

The custodian and source questionnaire: 43 questions in three parts

Use Part A with IT (and the MSP on the call), Part B with each key custodian, Part C as the team's sweep for what the first two miss. Record answers verbatim where possible; where an answer is an assumption rather than verified fact, mark it – the verified/assumed discipline Guide 10 formalises.

Part A · Infrastructure (IT / MSP) – 17 questions

1. What productivity platform do you run (M365 / Google / other), on what licence tier, and who administers it?
2. What email system, including archives, journaling, and any legacy servers from before a migration?
3. What happens, step by step, when an employee leaves – account, mailbox, OneDrive/Drive, licence, devices, and on what timetable?
4. What retention or auto-deletion policies apply to mail, Teams/Slack, files, and can they be suspended for named scopes?
5. What is the backup regime: what is backed up, how often, kept how long, rotated how, held where, by whom?
6. What audit logging exists (platform, file server, VPN, applications), and what is each log's retention window?
7. What file storage exists: servers, NAS, DMS, sync-and-share, and who controls permissions?
8. What line-of-business systems run the company (accounting, CRM, ERP, HR, ticketing), hosted where, exportable how?
9. What collaboration tools are licensed – and what do you know is used without being licensed?
10. What is the mobile-device policy: corporate, BYOD, MDM controls, remote-wipe triggers?
11. What CCTV, door-access and phone/VoIP systems exist, and their retention?
12. What third parties hold company data: MSP, hosting, former providers, developers, payroll?
13. What decommissioned systems, retired servers or stored media exist, and where physically?
14. Have there been migrations, ransomware events or major deletions in the relevant period?
15. Who can run tenancy-wide searches and exports, and has anyone already searched or exported anything for this matter?
16. What asset register exists for devices, and how accurate is it honestly?
17. What would you check that we have not asked about?

Part B · Per custodian – 15 questions

1. Which devices do you use for work – issued and personal – including tablets and home computers?
2. Where do your working documents live: local, OneDrive/Drive, shares, DMS, somewhere else?
3. Which messaging apps carry work conversations, with whom, and are any set to disappear?
4. Do you ever use personal email for work – forwarding, sending, receiving? (Ask for examples, not policy.)
5. What shared mailboxes, team channels or group chats are you in that touch these issues?
6. What systems do you use daily (CRM, finance, ticketing), and under whose login?
7. What do you keep on USB sticks or external drives, and where are they?
8. Have you deleted, archived or "tidied" anything relevant since the dispute arose – or been asked to?
9. What did you do with your previous phone and laptop?
10. Do you print and keep paper for anything relevant?
11. Who else would hold copies of the key exchanges – internally and at counterparties?
12. What calendars, notes apps or task tools record your work on these events?
13. Any recordings: calls, meetings, voicemails, dictation?
14. If you had to find the single most important document on these issues tonight, where would you look?

15. What are we going to find that you would rather explain now? (Ask it kindly; it is the highest-yield question on the list.)

Part C · The sweep – 11 questions for the team

1. Which departed employees held relevant roles, and what survives of their accounts and devices?
2. Which of the eight families has no entries on our map – and is that genuinely true or unasked?
3. What do the documents we already hold reference (systems, drives, apps) that the map lacks?
4. What do email signatures, headers and metadata reveal about tools in use?
5. Which counterparties, advisers and banks hold parallel records of the key events?
6. What group companies or overseas offices hold relevant data under different regimes (Guide 6; Guide 40)?
7. What contracts give rights over third-party-held data (inspection, audit, return clauses)?
8. What is on the corporate social accounts and website archive for the relevant period?
9. Whose personal devices matter under BYOD, and what is the legal route to them?
10. What physical evidence exists: papers, notebooks, whiteboard photos, stored media?
11. What has changed since the map was signed – new joiners, leavers, systems, incidents?

SECTION 21

Preservation and collection notes by family

Family	Preserve (week one)	Collect (when pursued)
1 · Endpoints	Quarantine, stop reissue/wipe; note asset register	Forensic image or targeted logical collection (Guides 31-33, 37); phones via forensic extraction (Guide 61)
2 · Email	Litigation hold incl. shared mailboxes; stop leaver deletion	Platform export or provider collection preserving metadata and folder structure (Guide 53)
3 · Cloud/collab	Suspend retention policies; export audit logs early	Purview/Vault or specialist collection; capture versions and permissions (Guides 51-59)
4 · File storage	Freeze snapshots/shadow copies; hold hardware disposal; capture permission listings	Targeted collection by folder with paths and timestamps intact (Guide 43)
5 · Structured	Stop decommissioning; confirm audit-trail retention; check SaaS contract clocks	Defined exports/queries with documented parameters; never ad-hoc spreadsheets alone (Guide 71)
6 · Messaging/social	Disable ephemerality (document it); preserve handsets before upgrades	Device extraction; platform archives; counterpart devices (Guides 63-67)
7 · Logs/physical	Same-day export requests: CCTV native export, auth/VPN logs, access-control	Native formats with player/codecs; hash on receipt (Guides 77-79)
8 · Backups/3rd parties	Pause rotation or preserve named sets; written notices to holders (Guide 29)	Restore-and-collect from defined sets; proportionality per Guide 49

Preservation and collection are different decisions with different price tags: preserving family 8 costs a letter and a paused rotation; collecting it costs restores and review. Keep the two columns separate in the map and in client advice.

SECTION 22

Privilege and confidentiality considerations

- **The map itself is work product.** Prepared for the litigation, the data map and interview notes attract litigation privilege. What you *publish* from it – DRD Section 2 answers, preservation confirmations – is methodology deliberately made open (Guide 17's share/hold line). Maintain the map in two layers from day one: the exhibitable inventory, and the privileged commentary.
- **Interview notes.** Custodian interviews conducted by lawyers for the litigation are privileged, but remember the limits of legal advice privilege after *Three Rivers (No 5)* for corporate clients: route interviews through the litigation-privilege frame (dominant purpose) and record that purpose.
- **Sources containing privileged material.** Flag on the map the sources rich in privileged content (GC's mailbox, board packs, advisers' folders) so collection and review workflows quarantine them (Guide 8's warning); the map is where privilege-protection planning starts.
- **Third-party mapping.** Preservation letters to third parties should not reveal strategy: ask for preservation of defined categories, not explanations of why they matter.
- **Confidential sources.** HR systems, payroll, medical and grievance files: map them, but plan confidentiality handling (redaction, clubs) before anyone collects.

SECTION 23

UK GDPR and data minimisation when mapping sources

Mapping is low-intrusion (an inventory processes little personal data), which is exactly why it should be complete: minimisation bites at *collection*, not identification. Under UK GDPR and the DPA 2018 (as amended by the Data (Use and Access) Act 2025), the practical rules:

- **Map everything, collect proportionately.** Article 5(1)(c) supports the pursue/park/release triage: parking a source with a dated proportionality note is minimisation in action, and reads well to both the court and the ICO-conscious client.
- **BYOD and personal accounts need a lawful, documented route.** Employee consent is rarely the right basis; legitimate interests with a balancing assessment, targeted scopes and, where feasible, custodian-assisted collection is the pattern (the series' BYOD tier: three bid-team phones, targeted, in Q2 2027).
- **Special-category caution.** HR, health and grievance sources go on the map with a handling plan, not into a general collection.
- **Transfers.** Overseas group companies and cloud regions raise transfer questions when collection starts (Guide 40 to come); note hosting locations on the map now.
- **Records.** The map plus the preservation log largely satisfies the accountability record for disclosure processing; date both.

SECTION 24

Proportionality: mapping everything, collecting selectively

The economics of the map are asymmetric. Identification costs hours; preservation of most sources costs configuration changes and letters; collection costs money per gigabyte; review costs money per document (Guide 19's cost anatomy). So the proportionality argument almost never justifies *not mapping*; it governs what you do with mapped sources.

Paragraph 6.4's factors are applied source by source at the triage stage (Figure 3, Q5): likely probative value, volumes, retrieval difficulty, cost. The map's honesty is what makes the argument credible: "we identified the backup vault, preserved the monthly sets, and propose not to restore them unless the live-source collections show gaps" (the classic *Digicel*-aware position) is a proportionality argument the court can accept – and the DRWG's 2026 survey results suggest scope discipline will only grow more central in the coming reforms.

THE STAGED-PROMISE PATTERN

The cheapest proportionate position on an expensive source is usually a preserved option plus a trigger: park it, preserve it, and define in the DRD the condition on which it gets opened (sampled richness, a gap in productions, a specific issue going live). Judges accept staged plans far more readily than flat refusals.

SECTION 25

Common mistakes and how to avoid them

Mistake	Consequence	Fix
Mapping only email and files	Structured systems, messaging and logs surface late; collections reopen	Force all eight families in every scoping (empty family = question)
Asking IT for a systems list and stopping	Shadow IT, personal accounts and habits invisible	Custodian interviews (Part B), lifecycle questions
Ordering work by importance, not volatility	CCTV, logs and rotations expire while mailboxes are debated	Figure 2 ladder sets sequence
Preserving without recording	Cannot later prove what was done when; certificate anxiety (Guide 16)	Dated preservation log per source
Ignoring leaver processes	Accounts and devices of the most relevant people destroyed on schedule	Leaver freeze for named individuals, day one
Treating backups as safety instead of sources	Rotation quietly deletes history weekly	Explicit pause/preserve decision, in writing
No third-party notices	MSPs and former providers purge on their own schedules	Guide 29 notices in week one
Shadow-mapping the opponent never	Their gaps discovered at production, too late to press	Section 18 mirror-map; preservation letter asks the family-8 questions
A map with no owner or version	Decays instantly; contradicts DRD later	Named owner, sign-off, change log
Confusing identification with collection in client advice	Client hears "map everything" as "pay for everything" and resists	Present the two price tags separately (Section 24)

SECTION 26

Technical limitations lawyers should understand

- **Inventories lie by omission.** Asset registers and CMDBs record what was procured, not what is used; reconciliation against network scans and interview answers is the provider's first job.
- **"Backed up" is not "restorable".** Backup software reports success against its own configuration; restore tests are the only proof, and old sets may need retired hardware or software to read.
- **Audit logs answer narrow questions.** Each log records the events it was configured to record, at the tier the licence pays for; absence of a log entry is weak evidence of absence of the act. Check coverage before promising conclusions.
- **Cloud "deletion" varies.** Recycle bins, retention holds, and versioning mean deleted rarely means gone (Guide 27) – but the recovery windows are product-specific and licence-specific; verify, never assume, per platform.
- **SaaS export is contract-limited.** What you can get out (fields, formats, histories, rate limits) is defined by the vendor's API and your tier; the "full export" sometimes is not.
- **Volatility figures are defaults, not laws.** Every retention window in this guide varies by configuration; the map must record the client's actual settings, verified in the admin console, not the product documentation's defaults.
- **Mapping disturbs nothing, but collection can.** Opening files changes access dates; previewing phones can alter state. Keep the mapping phase read-only and leave collection to defensible method (Guides 31-40).

SECTION 27

Questions lawyers should ask the opponent about their sources

1. What systems, platforms and repositories have you identified as holding potentially relevant documents, by our eight-family taxonomy or your own?
2. What retention and auto-deletion policies applied in the relevant period, and when and how were they suspended?
3. What is your backup regime, who operates it (any MSP or third party), and what preservation decision was taken about rotation – and when?
4. What audit logs exist (platform, file, authentication), what are their retention windows, and have you exported the relevant periods?
5. What happened to the accounts and devices of relevant leavers, with dates?
6. Which messaging applications carried relevant business communications, and what has been done about disappearing-message settings?
7. What personal accounts or devices are implicated, and what steps address them?
8. What legacy, migrated or decommissioned systems held relevant data, and what survives of them?
9. What third parties hold your data, and what preservation notices have you sent them?
10. Will you provide your data map or equivalent source inventory (in DRD Section 2 or otherwise), with dates of preservation steps?

Ask early, in the preservation letter and again in the DRD process. Late answers to early questions are the paper trail adverse-inference arguments are built from.

SECTION 28

Questions lawyers should ask a forensic or eDisclosure provider

1. Can you lead or support the mapping interviews, and do you have a questionnaire that merges with ours?
2. Which platforms in this estate have you collected from before, and where are the known traps (API limits, export formats, log tiers)?
3. Can you verify the client's actual retention and audit settings in the admin consoles, rather than relying on stated policy?
4. How quickly can you execute same-day preservation for volatile sources (CCTV export, log pulls, device quarantine)?
5. What is your method for preserving each family defensibly, and what documentation do you produce (method statements, hashes, chain of custody)?
6. How do you handle BYOD and personal-account collection so scope stays targeted and private material stays private?
7. What does preservation-only cost per source, versus collection, so we can price the pursue/park/release decisions?
8. Can you test-restore from the backup sets we propose to preserve, and what would restores cost if triggered later?
9. How will the map's outputs flow into processing and the DRD Section 2 answers without re-keying?
10. What in this estate would you escalate to a forensic examiner now rather than risk losing (artefacts, deleted data, disputed devices)?

SECTION 29

Suggested wording for instructions

A · INSTRUCTION TO CLIENT IT (day one)

"Pending further notice, and in respect of the individuals and systems listed in the Schedule: (1) suspend all automatic deletion, retention-expiry and archive-pruning processes; (2) suspend the leaver process for the listed individuals, including mailbox deletion, licence removal and device wiping or reissue; (3) pause backup rotation for the listed sets or preserve the current sets before rotation; (4) export and preserve the audit logs listed, covering [period], in native format; (5) make no attempt to review, open or tidy the preserved material. Please confirm each step in writing with the date and time it took effect, and tell us anything on the Schedule that cannot be done as asked."

B · PRESERVATION NOTICE TO A THIRD-PARTY HOLDER (MSP, former provider)

"We act for [client] in a dispute in which documents you hold or control on our client's behalf may be relevant. Until further notice, please preserve unaltered: (1) all backup sets, archives and snapshots relating to [client], including those subject to rotation or scheduled expiry; (2) all logs of administrative actions taken on [client]'s systems; (3) [specific categories]. Please confirm in writing the preservation steps taken, the date each took effect, and the retention schedule that would otherwise have applied. This request is made to preserve evidence; we will address access, restoration and costs separately."

C · MAPPING INSTRUCTION TO A FORENSIC / eDISCLOSURE PROVIDER

"We instruct you to assist in mapping [client]'s electronic evidence sources. Scope: (1) attend and technically lead interviews with IT and the custodians listed; (2) verify stated retention, audit and backup configurations against the relevant admin consoles; (3) produce a source inventory recording, per source: family, owner, contents, location, retention, volatility rating, preservation status and recommended collection method; (4) identify and execute urgent preservation for sources at risk within [30] days, reporting each step with dates; (5) flag any source requiring forensic handling before further access. Output: a data map suitable for DRD Section 2, and a preservation log suitable for exhibition."

D · DRD-FACING SOURCE STATEMENT (extract)

"The [claimant]'s documents are held in the following principal sources, identified through a mapping exercise completed on [date] and maintained since: [schedule by family]. Preservation steps, with dates, are set out at [reference]. The following identified sources are preserved but not proposed for search, for the reasons given: [schedule]. The [claimant] will review this position if [triggers]."

SECTION 30

Checklist: the source-mapping essentials

- ☐ Issues framed before mapping; map built issue-led
 - ☐ All eight families interrogated; any empty family treated as unanswered
 - ☐ IT/MSP interview done (Part A); actual settings verified in consoles, not policy documents
 - ☐ Key custodian interviews done (Part B), including personal-account and messaging questions
 - ☐ Sweep completed (Part C): leavers, legacy systems, third parties, counterparty copies
 - ☐ Every source volatility-rated; same-day actions executed for the top of the ladder
 - ☐ Leaver process frozen for named individuals; devices quarantined
 - ☐ Retention policies suspended in scope; suspension dates recorded
 - ☐ Backup rotation decision taken and documented
 - ☐ Audit logs exported for the relevant window before rolling off
 - ☐ Third-party preservation notices sent; confirmations chased
 - ☐ Closed sources (wiped, lost, expired) recorded with dates and alternative paths noted
 - ☐ Data map v1 signed off by client IT lead, dated, with named owner
 - ☐ Pursue / park / release decision recorded per source with reasons
 - ☐ Map versioned and maintained; feeds DRD Section 2 without re-keying
-

SECTION 31

Red flags

IN YOUR CLIENT'S ESTATE

- "IT is handled by someone who left" – or by an MSP nobody has called yet.
- Retention policies nobody can state; consoles nobody can access; an asset register that stopped in 2023.
- A key custodian's device recently "upgraded", "lost" or newly factory-reset.
- Tidying: folders reorganised, mail archived, chats cleared after the dispute arose.
- Business conducted visibly on WhatsApp or personal email while custodians deny it.
- A migration, rebrand or system decommissioning scheduled mid-dispute.
- Backup "success" reports for systems that no longer exist.

IN THE OPPONENT'S ANSWERS

- A source inventory that is all family 2 and 4: no logs, no structured systems, no messaging.
- Preservation "confirmed" without dates, scopes or named systems.
- Retention suspensions described in the future tense months into the dispute.
- Leaver accounts "unfortunately deleted in the ordinary course" for exactly the relevant people.
- Backups declared out of scope before anyone has asked what they contain.
- Third-party holders never mentioned despite an obviously outsourced estate.
- Answers that change between the preservation letter response and DRD Section 2.

SECTION 32

When to involve a digital forensic expert

- **Any source where user conduct is in issue.** If deletion, copying, exfiltration or backdating may be alleged, the mapping phase should end at the device door: quarantine and image before anyone else touches it (the Marsh laptop pattern).
- **Artefact-bearing endpoints.** Deciding whether a laptop needs full forensic imaging or targeted collection is itself an expert call, priced against the issues (Guides 32 and 37).
- **Log interpretation.** Audit-log tiers, coverage gaps and timestamp semantics (Section 26) are where confident lay readings go wrong; an examiner reports what a log can and cannot prove.
- **Fragile or failing media.** Old NAS boxes, retired servers, damaged drives: powering them up unadvised can be the last thing they do.
- **Recovery questions.** Whether the wiped phone's content survives anywhere (cloud backups, counterpart devices, carrier records) is a forensic reconstruction question, not a mapping one (Guides 27-28).
- **Method statements for the record.** Where preservation steps may later be challenged, an examiner's contemporaneous method statement (what was done, when, how verified) converts assertion into evidence.

SECTION 33

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

Forum	Source-mapping position
England & Wales, non-B&PC	CPR 31 and PD 31B: the reasonable-search factors (31.7) and PD 31B's technology questionnaire assume the same identification exercise; <i>Digicel</i> remains the governing caution.
Scotland	Recovery by specification and commission and diligence: no general duty to map for the opponent, but the same exercise is needed defensively (to preserve) and offensively (to draft precise specifications of what the other side holds).
Northern Ireland	Discovery under RCJ (NI) Order 24: broader relevance, affidavit-based lists; an incomplete estate map surfaces as a defective affidavit of documents, with professional consequences.
Arbitration	IBA Rules Art 3: production turns on requests for "narrow and specific" categories – drafting them requires a shadow map of the opponent's estate; your own map governs preservation and objections (burden, Art 9).
Employment tribunals	Disclosure by order under ET Rules; short timetables make volatility triage more, not less, urgent – CCTV and messaging evidence in dismissal disputes dies fastest.
Criminal proceedings	CPIA 1996: investigators must pursue all reasonable lines of enquiry, including those pointing away from the suspect – source identification is the statutory core; the AG's Guidelines (2024) address digital material scoping, and FSR Code obligations attach to forensic handling of what is seized.

SECTION 34

Glossary

Audit log	System record of user/admin actions: access, deletion, sharing, configuration changes.
BYOD	Bring your own device: personal hardware carrying business data.
CMDB	Configuration management database: IT's inventory of systems and assets.
Custodian	Person whose documents/communications are within scope; contrast non-custodial sources.
Data map	Dated, owned inventory of sources with retention, volatility and preservation status.
DMS	Document management system (iManage, NetDocuments): versioned document store with access logs.
DVR / NVR	Digital/network video recorder: CCTV storage, typically overwriting on short cycles.
Journaling	Automatic capture of every email sent/received into an immutable store.
MDM	Mobile device management: corporate control of phones, including remote wipe.
MSP	Managed service provider: outsourced IT operator, often holding backups and admin access.
NAS	Network-attached storage: shared storage appliance, common in smaller offices.
PST / OST	Outlook data files: local archives (PST) and cached mailbox copies (OST) on endpoints.
Retention policy	Automated deletion/archiving rules running on schedule.
Shadow IT	Tools in business use without IT governance or inventory.
Snapshot / shadow copy	Point-in-time image of a volume or system enabling historical recovery.
Volatility	Speed at which a source's evidence disappears under default settings.

SECTION 35

Authoritative UK references

- PD 57AD (paras 3.1-3.4 and 4: preservation; para 10.5 and Section 2: the DRD) and the Disclosure Review Document: [justice.gov.uk – PD 57AD](https://www.justice.gov.uk/pd-57ad); [DRD form](#)
- CPR 31.7 (reasonable search), 31.8 (control) and PD 31B (electronic documents questionnaire): [justice.gov.uk – CPR 31](https://www.justice.gov.uk/cpr)
- *Digicel (St Lucia) Ltd v Cable & Wireless plc* [2008] EWHC 2522 (Ch): [bailii.org](https://www.bailii.org)
- *Earles v Barclays Bank plc* [2009] EWHC 2500 (QB): [bailii.org](https://www.bailii.org)
- *Phones 4U Ltd v EE Ltd* [2021] EWCA Civ 116 (personal devices and third-party sources): caselaw.nationalarchives.gov.uk
- ICO, employment and monitoring guidance and UK GDPR resources: ico.org.uk; UK GDPR / DPA 2018 / Data (Use and Access) Act 2025: legislation.gov.uk
- Attorney General's Guidelines on Disclosure (2024), incl. digital material annexes: gov.uk; CPS disclosure guidance: cps.gov.uk
- Forensic Science Regulator statutory Code (v2, October 2025): gov.uk/fsr
- IBA Rules on the Taking of Evidence in International Arbitration (2020): ibanet.org
- Law Society practice notes on disclosure and on generative AI in disclosure (Nov 2025): lawsociety.org.uk

Links current at re-issue (September 2026). Retention windows and licence tiers cited in this guide are illustrative defaults: verify your client's actual configuration.

SECTION 36

How a specialist laboratory can assist

Source mapping rewards technical fluency applied early. A specialist electronic disclosure and digital forensics laboratory can:

- **Run the mapping sprint:** lead the IT and custodian interviews with the Section 20 questionnaire, verify real settings in the admin consoles, and deliver a signed-off data map inside the first fortnight.
- **Execute volatility-first preservation:** same-day CCTV and log exports, audit-log pulls before rolling windows close, device quarantine and imaging, retention suspensions confirmed in writing.
- **Handle every family defensibly:** from tenancy-wide cloud preservation to NAS snapshots, SaaS exports within contract limits, and forensic extraction of phones and messaging apps.
- **Produce the record:** method statements, hash manifests and preservation logs that turn "we acted properly" into evidence – and flow straight into DRD Section 2.
- **Shadow-map the opponent:** metadata and header analysis, estate inference, and the precise preservation-letter questions that surface MSPs and backup vaults early.
- **Advise the pursue/park/release economics:** per-source preservation and collection pricing so proportionality decisions are made on numbers.

NPCC-aligned digital evidence handling, ISO 17025 aligned practice, and examiners who have defended their maps in court. The earlier the laboratory joins, the shorter the ladder's casualties list.



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