COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

How to Build a Defensible eDisclosure Strategy at the Start of a Case

From Pleadings and Issues to Collection and Review Protocols

Defensibility is built, not retrofitted. This guide provides the step-by-step workflow for the first weeks of a disputed matter: extracting issues from the pleadings, preserving on day one, mapping sources and custodians, analysing control, triaging forensic risk, measuring the estate, designing the search, taking a position in the DRD, and closing with the collection plan and review protocol that the whole exercise will be judged against.

⏱ Estimated reading time: 30 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its eDiscovery arm, **e-discovery.uk**, is instructed at exactly the moment this guide addresses: the start, when the chain of custody opens, preservation and identification are logged as the first entries, and every later phase closes on its own defensibility checkpoint (what was done, by whom, when, against which hash, under whose instruction). This guide is the whole of that discipline compressed into a workflow, and it draws together the companion guides in this series on sources, custodians, control, searches and early assessment.

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

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: WHAT MAKES A STRATEGY DEFENSIBLE

A defensible eDisclosure strategy is a written plan, made at the start, that connects every scope and method decision to the pleaded issues, preserves first and decides second, measures before committing, builds the forensic escalation path in from day one, and generates its own evidence as it executes (data map, hold register, control schedule, assessment report, search protocol, collection logs, review protocol). Defensibility is built, not retrofitted: the exercise that can produce its plan and its records answers every later challenge with a document; the exercise that improvised answers with recollection.

- **The workflow has ten steps and a strict opening order.** Issues first (they drive everything), preservation immediately (it cannot wait for the plan), then identification, custodians, control, forensic triage, assessment, search design, the procedural position, and finally the collection plan and review protocol that operationalise it all.
- **Preservation and planning run in parallel, never in sequence.** The single most common strategic failure is letting volatile data die while the strategy is drafted. Day-one actions are listed in Step 2 and they precede every other judgment.
- **Measure, then negotiate.** The strategy takes its DRD and budget positions from measured numbers (Step 7's assessment) and tested terms (Step 8), which converts negotiation from assertion into arithmetic and is itself a mark of defensibility.
- **The strategy is a living governed document.** It has an owner, a cadence, version control and change triggers, because pleadings amend, review finds things, and a strategy that cannot absorb change silently stops being followed.
- **This guide integrates the series.** Each step points to the companion guide that covers it in depth: sources (*Finding the Evidence*), custodians, control, forensic triage (*eDisclosure or Digital Forensics?*), assessment, search design, and the lifecycle (*The EDRM for UK Litigation Teams*).

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: strategy or improvisation

Every disclosure exercise gets a strategy; the only question is whether it is written at the start or reverse-engineered at the end. The improvised version is recognisable in any war story: preservation that started when someone remembered; custodians chosen in a meeting nobody minuted; terms agreed under CMC pressure and regretted for a year; a certificate signed against a search no one can fully describe; and, when challenged, a scramble through emails to reconstruct why anything was done. None of it is misconduct; all of it is expensive, and some of it is dangerous, because the disclosure certificate is personal and the court's patience with process failures is short.

The written version costs a fortnight of structured work at the start and repays it continuously: scope negotiations arrive with evidence, budgets survive scrutiny, the team executes against protocols instead of memory, mid-case surprises route down a pre-built escalation path, and the challenge that eventually comes (it usually does, from one direction or the other) is answered by producing documents that already exist. The ten steps that follow are that fortnight, in order, with each step's outputs named, because in this subject the outputs are the strategy.

§ 0 3 · WHY IT MATTERS LEGALLY

Why the first weeks matter legally

- **Duties begin at contemplation, not issue.** PD 57AD's preservation duties (suspend deletion, notify employees and relevant former employees and third parties, obtain written confirmation) attach when proceedings are contemplated, and legal representatives carry personal obligations to take reasonable steps. The strategy's Step 2 is the discharge of live duties, not preparation for future ones.
- **The procedural documents assume the work is done.** Initial Disclosure accompanies statements of case; the DRD requires issue lists, source descriptions, volumes, proposals and cost estimates; PD 31B expects informed pre-CMC discussion. Each is a deadline that the ten steps feed, and each is painful exactly in proportion to how much of the workflow was skipped.
- **The certificate is the strategy's final exam.** The disclosure certificate and statement describe the search and its limits, personally. A signatory with the strategy file signs a summary of records; without it, an assertion.
- **Costs consequences accrue early.** Precedent H is filed early and revised only with justification; adverse conduct findings (late preservation, silent narrowing, obstruction) trace back to first-month decisions; and proportionality arguments are won by whoever brings numbers, which the strategy manufactures on schedule.
- **Criminal and regulatory matters compress the same workflow.** Reasonable lines of enquiry, Disclosure Management Documents and regulator deadlines are the same steps under sharper clocks; the workflow transfers with the vocabulary adjusted.

§ 0 4 · THE MAP

The workflow at a glance

Figure 1 · Ten steps. Step 2 fires on day one regardless of everything else; Steps 3 to 6 overlap heavily in week one; Steps 7 and 8 occupy weeks two and three; Steps 9 and 10 land before the deadlines they serve. The arrows also run backwards: review findings reopen custodians, assessment reopens sources, and the strategy document versions each change.

WHEN	WHAT IS DONE	WHAT EXISTS AT THE END
Day 1	Step 2 in full; Step 1 begun; provider and (where triggered) forensic examiner engaged	Hold issued and logged; timers suspended; leaver pipeline frozen; third-party notices out
Week 1	Steps 1, 3, 4, 5, 6: issues matrix, interviews, data map, tiered custodian list, control schedule, triage decisions; volatile and trigger-positive sources forensically preserved	The evidential skeleton: every source and holder mapped, labelled and preserved or escalated
Weeks 2–3	Steps 7 and 8: assessment levels 1 to 3, scenario modelling, term testing, search protocol drafted	The assessment report and tested search design
Pre-CMC	Steps 9 and 10: DRD and EDQ drafted from the records, budget aligned, collection plan and review protocol finalised	The strategy document, complete, with every annex it will ever need to produce

§ 0 5 · STEP 1

Pleadings to issues: the issue-source matrix

Purpose: everything downstream (custodians, ranges, sources, terms, Models) is justified by reference to the issues, so the issues are extracted first, precisely, from whatever exists: statements of case if served, pre-action correspondence and instructions if not.

Actions: draft the working Issues for Disclosure early (they will be negotiated later, but the internal version drives the strategy now); decompose each issue into the events and decisions behind it; and build the **issue-source matrix**: issue → events → likely roles and people → likely systems and channels → date anchors. One page per issue is enough; the discipline is the mapping, not the prose. Where the client is claimant, do this before proceedings are drafted, because the pleading itself improves when someone has mapped what the documents will show.

Outputs: working issues list; issue-source matrix; first-cut date anchors per issue.

Common failure: starting from the data ("collect the mailboxes, we will work out relevance later"), which produces scope without justification and review without direction. The matrix is twenty lines of thought that saves twenty thousand documents of drift.

§ 0 6 · STEP 2

Day-one preservation

Purpose: discharge the live duties and stop the estate shrinking while it is being studied. This step does not wait for Steps 1 or 3 to finish; it runs on day one with whatever is known, and widens as knowledge arrives.

Actions: issue the written legal hold to all plausible custodians and to IT operations, with acknowledgment tracking; suspend auto-deletion and retention timers in-platform (mail, chat, recycle bins); freeze the leaver pipeline (no account deletions, no device reissue) and pull known leavers' devices from circulation; pause backup rotations for in-scope systems; send preservation notices to third parties holding client data (MSPs, hosts, processors) and, where relevant, to former employees; disable disappearing-message settings on identified channels, in writing; and open the hold register that records all of it with dates.

Outputs: hold notice and register; platform-suspension confirmations; third-party and former-employee notices; the client's written preservation confirmation that PD 57AD requires.

Common failure: a hold that reaches people but not systems: the notice acknowledged by every custodian while the 90-day chat timer runs on and the storeroom laptop is reissued on schedule. The register exists to prove the systems were reached too.

§ 0 7 · STEP 3

Identification: the data map

Purpose: establish where evidence could exist, across the whole modern estate: endpoints, communications (including messaging apps and collaboration platforms), storage and backups, business systems, ambient sources (CCTV, access control, telephony, vehicles), logs, and third-party holdings.

Actions: run the dual-track interviews (custodians and IT separately, compared afterwards); issue the written questionnaires; execute the completeness cross-checks (accounts-payable review for the SaaS estate, SSO application lists, device reconciliation, sampling of first-collected data); and build the versioned **data map**: source → custodian or system owner → location → volume → volatility → decision → reason. Our companion guide *Finding the Evidence* provides the full source taxonomy, the volatility league table and the three-part questionnaire this step deploys.

Outputs: data map v1 with reasoned inclusions and exclusions; signed questionnaire returns; cross-check results; an updated hold (Step 2 widens to whatever identification found).

Common failure: interviewing IT only. The systems view never contains the shadow estate (the WhatsApp thread, the personal drive, the departmental tracker) where the candid material lives.

§ 0 8 · STEP 4

Custodian selection and tiering

Purpose: convert the issue-source matrix and the data map into a defensible, proportionate custodian list.

Actions: resolve roles to named people across the whole period (including predecessors and leavers); run every candidate through the four-question tiering tree (core / targeted / preserve-only / reasoned exclusion); build the identity table per custodian (all addresses, aliases, domains); list non-custodial sources (shared mailboxes, repositories, organisational systems) independently with named system owners; and record every exclusion with a one-line reason. The method, the difficult categories and the interview set are in the companion guide *Identifying the Right Custodians*.

Outputs: tiered custodian list with rationales; identity tables; system-owner assignments; interview records.

Common failure: the org-chart list: seniority instead of participation, six directors and no project coordinator, later embarrassed by correspondent analysis (which Step 7 will run in any event, so run it for yourself first).

§ 0 9 · STEP 5

Control analysis and third parties

Purpose: establish, per holder, whether documents are within the client's control (possession, right, or arrangement in fact) and choose the route to everything that matters but is not.

Actions: map tenancy and domain administration across the group; gather and read the operative contracts (intra-group, MSP, SaaS, employment and BYOD, contractor); run each holder through the control decision tree; issue the structured personal-device requests to custodians who used personal channels, under a privacy-protective protocol; and select third-party routes (voluntary request, CPR 31.17, witness summons, *Norwich Pharmacal*, letters of request) for the genuine strangers. Build the **control schedule**: holder → basis → action → response. The law and the drafted wording are in the companion guide *Control of Electronic Documents*.

Outputs: control schedule; issued requests and notices with responses tracked; third-party route plan with lead times.

Common failure: control positions asserted before the facts are gathered: "the subsidiary's documents are not ours" from a client whose IT team administers the subsidiary's mailboxes.

§ 10 · STEP 6

Forensic triage

Purpose: decide, per source, whether ordinary collection is sufficient or forensic preservation or examination is required, before anything is touched in a way that forecloses the choice.

Actions: run every source against the forensic triggers (disputed authenticity, suspected deletion, leavers under a cloud, chronology anomalies, contested attribution, central mobile chat, locked or damaged sources, criminal or regulatory exposure); forensically acquire everything trigger-positive or volatile now, deferring examination until questions crystallise (the image supports every later strategy; an ordinary export forecloses some); and write the **escalation paragraph** into the case plan so that anomalies found later route to preservation, not to an IT "quick look". The full decision tree and the ten triggers are in the companion guide *eDisclosure or Digital Forensics?*.

Outputs: per-source triage record; forensic acquisitions with chain-of-custody logs; the standing escalation protocol; scoped examination instructions where questions already exist.

Common failure: treating triage as a later decision. It is a day-three decision at the latest, because the sources it protects are exactly the ones ordinary handling contaminates.

§ 11 · STEP 7

Early data assessment

Purpose: measure before committing: volumes, per-custodian footprints, file types, duplication, communication patterns, privilege concentration and the likely relevant core, so that Steps 8 and 9 negotiate and budget on numbers.

Actions: pull in-place platform statistics across the estate; collect and index a deliberate seed (core custodians plus the key repository) under full chain of custody; run the seven estimates; test candidate terms with hit reports and sampled relevance; model the review population and cost per scenario on the table; and label every source promote / stage / park / escalate. The workflow, the report contents and a worked example with numbers are in the companion guide *Early Data Assessment Before Disclosure Costs Escalate*.

Outputs: the assessment report with tolerances stated; scenario models; anomaly flags handed to the Step 6 escalation path; the evidence pack for every scope negotiation to come.

Common failure: skipping assessment to save a fortnight, then spending it three times over in renegotiated terms, revised budgets and processing that the numbers would have parked.

§ 1 2 · STEP 8

Search design

Purpose: set the seven levers of a reasonable search (custodians, ranges, sources, keywords, analytics, proportionality, sampling) deliberately, and write them into a versioned search protocol.

Actions: anchor per-issue date ranges to the matrix's events (checked against Step 7's timelines); divide the source list into searched, preserved-only and excluded with reasons; build terms from the data's vocabulary (a core-document sample read comes first) and test every term with hit reports and sample reads before agreement; set the analytics defaults (dedupe scope, threading, near-duplicates) and make the TAR decision on numbers; and write the sampling and validation plan, including the null-set sample that will justify stopping. The craft, the failure examples and the negotiation method are in the companion guide *What Is a Reasonable Electronic Search?*.

Outputs: the search protocol v1; exchanged-ready term proposals with hit data; the validation plan.

Common failure: terms agreed before terms tested, under CMC time pressure, producing populations the timetable cannot absorb. Step 7 exists so this step never negotiates blind.

§ 1 3 · STEP 9

The procedural position: DRD, Models, budget

Purpose: convert the accumulated records into the party's public position: the DRD (or EDQ), the Model proposals per issue, and a costs budget the numbers support.

Actions: draft DRD Section 1 from the working issues list and Section 2 from the data map, custodian list, control schedule and assessment tables (the sections almost write themselves when the steps were run); propose Models per issue with the measured cost of each alternative; state staging and reasoned exclusions openly with their evidence annexed; align Precedent H's disclosure phase with the scenario the DRD proposes, on the same numbers; and prepare the negotiation posture: what is offered (preserve-only for marginal custodians, staged tranches, tested-term exchanges) and what is resisted, with the data that resists it.

Outputs: DRD / EDQ drafts with annexes; budget aligned to the proposed scenario; a negotiation brief for the CMC.

Common failure: the DRD written from memory in the week before the CMC, describing an exercise subtly different from the one the records show, a divergence opponents are increasingly good at finding.

§ 1 4 · STEP 10

Collection plan and review protocol

Purpose: close the strategy with the two operational documents the execution phase runs on, so that what was designed is what is done.

Actions, collection plan: per source, the method (platform export under protocol, targeted forensic collection, extraction level for mobiles, report-based export for structured systems), the operator, the schedule, and the logging standard (hash manifests, collection logs, chain of custody throughout); self-collection prohibited in terms; promotion mechanics from the assessment seed confirmed so nothing is re-done.

Actions, review protocol: the issue list and coding rules; privilege guidance and the contemporaneous log; QC and sampling regime; TAR training and validation procedure from the Step 8 plan; confidentiality and redaction rules; the production specification agreed early (formats, metadata fields, families, natives) so review codes toward it; and the escalation paragraph from Step 6, verbatim, so every reviewer knows that anomalies stop, log and route.

Outputs: the collection plan; the review protocol; the production specification; provider instructions incorporating all three.

Common failure: review begun before the protocol is settled, so early coding is redone; and production format left to the exchange fortnight, so spreadsheets flatten and families break at the last, most expensive moment.

§ 1 5 · THE ARTEFACT

The strategy document and its governance

The strategy document is the master file that assembles the ten steps' outputs, and it needs only a disciplined table of contents:

SECTION	CONTENTS (THE STEP OUTPUTS, FILED ONCE)
1 · Issues	Working Issues for Disclosure; the issue-source matrix; date anchors
2 · Preservation	Hold notice and register; suspensions; third-party and leaver notices; client confirmation
3 · Sources	Data map (versioned); questionnaire returns; cross-check results
4 · Custodians	Tiered list with rationales; identity tables; system owners; interview records
5 · Control	Control schedule; requests and notices with responses; third-party route plan
6 · Forensic	Triage record; acquisition logs; the escalation protocol; examination scopes
7 · Assessment	The assessment report and scenario models
8 · Search	Search protocol; term proposals and hit reports; validation plan
9 · Procedure	DRD / EDQ drafts and annexes; budget alignment; negotiation brief
10 · Execution	Collection plan; review protocol; production specification; provider instructions

Governance is four short rules. An **owner**: one named lawyer owns the document and the certificate consequences; providers execute, the owner decides. A **cadence**: a weekly checkpoint against the provider's report (volumes, exceptions, QC, deviations), minuted in one paragraph. **Change control**: amendments to pleadings, added custodians, promoted tranches and protocol deviations are versioned into the document with a dated reason, because a strategy that absorbs change visibly stays defensible and one that changes silently stops being a strategy. And a **single client point of contact** for IT actions, so preservation and collection instructions have one accountable channel.

§ 16 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Sequencing preservation behind planning.** The fortnight of careful strategy during which the CCTV overwrote and two laptops were reissued.
- **Scope before issues.** Collecting "the obvious mailboxes" before anyone wrote down what the case is about, then justifying the scope backwards.
- **The unwritten strategy.** Decisions made well but recorded nowhere, indistinguishable years later from decisions never made.
- **Negotiating blind.** DRD positions and budgets set before assessment, then defended out of consistency rather than evidence.
- **The missing escalation path.** The anomaly spotted in week two of review and mentioned in week nine, after the source was reprovisioned.
- **Protocols after the fact.** Review protocols written to describe what reviewers were already doing; collection "protocols" reconstructed for the certificate.
- **Strategy as a one-time event.** The document finished, filed and never versioned, while the case moved on without it.
- **Client self-help.** The well-meaning client who "got a head start" by exporting mailboxes and browsing the leaver's laptop before instruction; the strategy's first week then includes damage assessment.

Technical limitations

- **The plan meets the estate.** Licence tiers, export-tool gaps, provider log windows and platform quirks constrain what any strategy can promise; Steps 3 and 7 exist to discover the constraints before the DRD asserts through them.
- **Estimates stay estimates.** Assessment numbers carry tolerances; the strategy states ranges and the DRD inherits them, because exact counts asserted early become completeness arguments later.
- **Preservation cannot resurrect.** Day-one action protects what exists on day one; where the client arrives late, the strategy documents what was already lost and why, which is itself the defensible position.
- **Protocols bind people imperfectly.** Review protocols and escalation paragraphs work through training and QC, not existence; the weekly cadence is where drift is caught.

§ 17 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording for instructions

Ask your client, on day one

- What deletion is scheduled to happen this week, on any system, to anyone's account or device?
- Who has left or is leaving, and where are their accounts and devices right now?
- Who can suspend retention timers today, and who will confirm in writing when it is done?
- Has anyone already collected, exported, examined or tidied anything since the dispute arose?
- Who is the single point of contact for every IT action from now on?

Ask your opponent, through the process

- When did your preservation steps take effect, item by item, and what automated deletion ran before them?
- Provide your data map's substance: sources considered, included and excluded, with reasons.
- What assessment underlies your proposals, and will you exchange volumes, counts and tested terms?
- What are your collection methods per source, and will logs and hash manifests be available?
- What is your review methodology, validation plan and production specification?

Ask an eDiscovery / forensic provider, at engagement

- Can you mobilise Step 2 support and volatile-source preservation this week, and what does that cost?
- Which steps do you deliver in-house (interviews, assessment, forensic acquisition, processing, hosting, review support), and where are the hand-offs?
- What per-step deliverables do we receive (logs, manifests, reports, protocols), and can we see specimens?
- How does assessed data promote into processing, and how are suppressions logged and reversible?
- Who from your side attends the weekly checkpoint, and who would give factual or expert evidence if methodology were challenged?

SUGGESTED WORDING · ENGAGEMENT INSTRUCTION TO A PROVIDER (CORE PARAGRAPHS)

> "You are instructed to support the disclosure exercise in [matter] in accordance with the strategy document at Annex A, as versioned from time to time. Immediate actions (within 2 working days): support implementation of the preservation steps at Annex A section 2, and forensically acquire the sources listed at Annex A section 6 under full chain of custody. Thereafter: identification support and early data assessment per sections 3 and 7; search-term testing and protocol support per section 8; collection per the collection plan at section 10, with hash manifests and collection logs delivered per source; processing under the processing protocol, with volumes reported in and out of each step, exceptions logged and resolved, and all suppressions logged and reversible; hosting and review support under the review protocol. You will provide a weekly written checkpoint report and will notify us within one working day of any integrity, completeness or forensic concern. No collected data is to be deleted, and no deviation from the annexed protocols is to occur without our written agreement."

SUGGESTED WORDING · THE ESCALATION PARAGRAPH (FOR THE REVIEW PROTOCOL AND CASE PLAN)

> "Any team member or provider identifying material suggesting deletion, fabrication, alteration, backdating, unauthorised transfer or other integrity concern shall record the concern in the escalation log and take no further investigative step. The implicated source shall not be accessed further. Supervising counsel will determine within 48 hours whether forensic preservation or examination is required, and until that determination no person other than the instructed forensic examiner shall access the implicated source, device or account."

§ 18 · QUICK CONTROL

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

The strategy checklist

- ☐ Day one: hold issued and registered; timers suspended; leaver pipeline frozen; third-party notices sent; IT single point of contact named
- ☐ Issues extracted and the issue-source matrix built before scope decisions
- ☐ Data map v1 from dual-track interviews and cross-checks, exclusions reasoned
- ☐ Custodians tiered with rationales; identity tables built; system owners named
- ☐ Control schedule completed; personal-device requests issued under protocol; third-party routes planned
- ☐ Forensic triage run per source; trigger-positive and volatile sources acquired; escalation paragraph adopted
- ☐ Assessment report delivered with tolerances; every source labelled promote / stage / park / escalate
- ☐ Search protocol written; every term tested before agreement; validation plan set
- ☐ DRD / EDQ and budget drafted from the records, on the same numbers
- ☐ Collection plan and review protocol finalised; production specification agreed early; self-collection prohibited
- ☐ Strategy document assembled, owned, versioned; weekly checkpoint cadence running

Red flags

- Any week-one sentence beginning "once we have decided the strategy, we will preserve".
- Scope discussions with no issues list on the table.
- A client who has "already pulled everything off the server to help".
- DRD numbers nobody can trace to a measurement, on either side.
- Terms proposed or agreed that have never met a hit report.
- No escalation route anyone can name when asked.
- A strategy document whose version history stops at v1.
- Protocol deviations discovered at the checkpoint and minuted nowhere.

When to involve a digital forensic expert

Within this workflow, the forensic hand-offs are built in: Step 2 where volatile or suspect sources need same-week laboratory preservation; Step 6's triage for everything trigger-positive (authenticity, deletion, attribution, exfiltration, locked or damaged sources, criminal or regulatory exposure); Step 7's anomalies (timeline gaps, encrypted clusters, footprints that contradict the account); and any later escalation-log entry. The governing principle is asymmetry: forensic acquisition now preserves every later option, ordinary handling forecloses some,

so uncertainty resolves toward preservation. The full triage discipline is in *eDisclosure or Digital Forensics? Choosing the Correct Approach*.

§ 19 · COMMON QUESTIONS

Frequently asked questions

What makes an eDisclosure strategy "defensible"?

Three properties. Connection: every scope and method decision traces to the pleaded issues through the matrix, the tiering and the protocol. Evidence: decisions rest on measured numbers and tested terms, not instinct. Records: the strategy generates its documents as it executes (hold register, data map, control schedule, assessment report, search protocol, logs), so any later challenge is answered by production, not reconstruction. A strategy with those properties can be wrong in places and still defensible; a strategy without them can be right everywhere and still indefensible.

How early is early? The dispute has only just surfaced.

Step 2 is due the day proceedings are contemplated, which is usually before anyone calls it litigation. Steps 1 and 3 to 6 belong in the first fortnight even pre-action: preservation duties are live, pre-action protocols reward preparedness, and pre-action assessment (Step 7) improves pleading and settlement judgment. Nothing in the workflow waits for issue of proceedings; the CMC merely collects its outputs.

Our client already collected data themselves. Is the strategy compromised?

Damaged, not doomed. Record exactly what was done, by whom, when and with what tools; stop further self-help immediately; assess with the provider what the informal collection preserved and destroyed; re-collect defensibly where sources still allow it; and route anything trigger-positive to forensic assessment of the handling itself. Candour in the DRD about the early handling, with the remediation documented, is a survivable position; discovery of it by the opponent is not.

Does a small case need all ten steps?

It needs all ten questions answered; the answers are just shorter. A two-custodian employment dispute can run Step 2 in an afternoon, Steps 3 to 6 in two meetings, Step 7 at level 1 only, and Steps 8 to 10 in a five-page protocol. What small cases cannot safely skip is the same as large ones: day-one preservation, reasoned scope, tested terms and a written record.

What happens to the strategy when the case changes?

It versions. Amended pleadings re-run Step 1's matrix; new custodians re-run Steps 4 to 6 for the additions; staged tranches promote on their defined triggers; and each change is dated and reasoned in the document. The living-document commitment belongs in the DRD itself, because promptly proposed, well-recorded changes read as diligence while silent ones read as concealment.

Who should build the strategy: the firm, the client or the provider?

The firm owns it (the certificate and the court-facing assertions are the lawyers'); the client supplies the facts and a single accountable IT channel; the provider contributes the measurement, the technical constraints and the execution machinery, and a good one will challenge the plan where the estate cannot support it. What fails is delegation of the whole to either of the other two: client-built strategies inherit self-collection risks, and provider-built ones optimise for workflow rather than for the case.

§ 20 · REFERENCE

Glossary

Change control
The discipline of versioning the strategy with dated, reasoned amendments as the case moves.

Checkpoint report
The provider's weekly account of volumes, exceptions, QC and deviations, reviewed at the governance cadence.

Collection plan
The per-source schedule of method, operator, timing and logging standard for all collection.

Escalation paragraph
The standing instruction that integrity anomalies stop work, get logged and route to counsel within 48 hours.

Hold register
The dated record of hold recipients, acknowledgments, suspensions and releases.

Issue-source matrix
The Step 1 mapping of each issue to events, roles, people, systems and date anchors.

Preserve-first asymmetry
The principle that forensic acquisition keeps every later option open while ordinary handling forecloses some; uncertainty resolves toward preservation.

Production specification
The agreed formats, metadata fields and family rules that review codes toward from the start.

Review protocol
The written rules of review: issues, coding, privilege, QC, validation, redaction and escalation.

Search protocol
The versioned design of the search: scope, tested terms, analytics and the validation plan.

Strategy document
The owned, versioned master file assembling the ten steps' outputs.

Tiering
Grading custodians (core, targeted, preserve-only, excluded with reasons) so effort matches involvement.

Sources and authoritative references

The workflow in this guide draws on materials published by our e-discovery practice and laboratory, referenced here as sources:

- e-discovery.uk, the practice's method statement ("Bring us in early. Defensibility is built, not retrofitted") and per-phase defensibility checkpoints across the EDRM: e-discovery.uk
- e-discovery.uk, EDRM phase notes: Identification, Preservation, Collection, Processing, Review and Production: e-discovery.uk/edrm/identification (and the linked phase pages)
- e-discovery.uk, Knowledge Centre practice notes, including search-term negotiation and mobile evidence: e-discovery.uk/knowledge
- cflab.uk, digital forensics services and the five-stage laboratory workflow (identification, preservation, acquisition, examination, reporting) that Steps 2 and 6 hand into: cflab.uk/digital-forensics-services
- cflab.uk, guides for lawyers, including the treatment of preservation best practice and forensic triggers: cflab.uk/guides
- Practice Direction 57AD (preservation duties; Initial and Extended Disclosure; the DRD and Models): justice.gov.uk, PD 57AD
- CPR Part 31 and PD 31B (reasonable search; pre-CMC discussion; the EDQ): justice.gov.uk, PD 31B
- CPR Part 3 (costs management and Precedent H): justice.gov.uk, Part 3
- CPR Part 35 (experts) and CrimPR Part 19: justice.gov.uk, Part 35
- Attorney General's Guidelines on Disclosure (rev. 2024, digital material and Disclosure Management Documents): gov.uk, AG's Guidelines

- ICO, UK GDPR guidance: ico.org.uk · Data Protection Act 2018: legislation.gov.uk/ukpga/2018/12 · Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/21

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

This workflow is our standing offer: bring us in early, because defensibility is built, not retrofitted. On engagement we support Step 2 the same week (volatile-source preservation under laboratory chain of custody, platform suspensions, leaver-device acquisition), then deliver the measurement and machinery the strategy runs on: identification support and the questionnaires, early data assessment with promotion into processing, tested search design with exchange-ready hit reports, per-source collection to the standard each source's risk demands, processing with reversible, audited culling, Relativity-ready hosted review under your protocol, and productions to the agreed specification with manifests exchanged. The laboratory receives every escalation this guide builds in (triage-positive sources, assessment anomalies, review-stage flags) and reports under CPR Part 35 / CrimPR Part 19 where opinion evidence is needed. One team, one chain of custody, weekly checkpoints, and candid advice, including where a step can safely be done by your own team. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace