



CFL ELECTRONIC EVIDENCE SERIES · PRACTICAL DIGEST

Ten Practical eDiscovery Guides, One Page Each

The most important points of ten guides from the e-discovery.uk library, condensed into one A4 sheet apiece with the workflows, decision ladders and evidence maps that lawyers actually use. Written for solicitors, barristers, in-house counsel, disclosure lawyers, investigators and litigation-support professionals in England and Wales.

Prepared by Computer Forensics Lab E-Discovery Team

01 The First eDisclosure Meeting: 50 Questions Lawyers Should Ask

Electronic disclosure practice · Part 1 fundamentals

03 Early Data Assessment Before Disclosure Costs Escalate

Costs and early case assessment

05 How to Design Defensible Keyword Searches

Search terms and technology assisted review

07 How to Draft an Electronic Disclosure Production Protocol

Production and redaction

09 Investigating Suspected Employee Data Theft

Data theft and exfiltration · Departing employees

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

Electronic disclosure practice · Part 1 fundamentals

04 Completing the Disclosure Review Document: A Technical and Legal Guide

Disclosure and PD 57AD

06 Should Backup Systems Be Searched for Disclosure?

Electronic disclosure practice · Preservation

08 Digital Redaction That Cannot Be Reversed

Production and redaction

10 Preserving Evidence After a Cyber-Attack or Ransomware Incident

Cyber incidents and ransomware · Preservation

COMPUTER FORENSICS LAB · CFLAB.UK · E-DISCOVERY.UK

Each sheet condenses a full guide (17 to 27 pages) available free at e-discovery.uk/library. The worked examples are fictional. This publication provides general information as at September 2026 and is not legal advice; it does not create a professional relationship and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Where rules differ in Scotland, Northern Ireland, arbitration, tribunals or criminal proceedings, the full guides identify the differences.



Scan to save our contact details

The First eDisclosure Meeting: 50 Questions Lawyers Should Ask

One-page guide 1 of 10

Condensed from the full CFL guide
(23 pages, e-discovery.uk library)

One meeting, ten themes, and the 48-hour rule that decides whether evidence survives the first fortnight.

THE HEADLINE POINT

The first eDisclosure meeting is not a fact-finding chat. It is the moment the client's data landscape is mapped, the preservation gaps are found, and the clock on rolling retention is stopped. Ask fifty questions in ten themes, grade every answer as verified or assumed, and confirm within 48 hours what has been suspended.

01 Ten themes the first meeting must cover (Parts A to J)

A · Context Dispute, issues, period in play, who was involved, what already exists on paper.	B · IT architecture Tenant, email platform, file stores, line-of-business systems, who administers them.	C · Custodians and devices Named people, roles, laptops, phones, leavers, reissued kit.	D · Cloud and SaaS M365 or Workspace, DMS, CRM, project tools, personal cloud in use.	E · Retention, deletion, backups Purge schedules, audit-log windows, backup rotation, leaver process.
F · Preservation already taken Holds applied, dates, who told whom, what is still running.	G · BYOD and messaging WhatsApp, Signal, Teams chat, disappearing-message settings, personal phones.	H · Third parties and control MSPs, group companies, agents, inspection rights, contractual reach.	I · Privacy and privilege Special-category data, employee monitoring limits, in-house legal channels.	J · Logistics Who owns the next 48 hours, provider access, budget signals, decision log.

02 Before, during and after: the meeting as a preservation event

1 Before Send the client a short pre-meeting note. Invite the IT lead, not only the general counsel. Read the pleaded period and list the systems you expect to hear about.	2 During Work Parts A to J in order. For every answer record V (verified) or A (assumed). Seven of the fifty questions are time-critical: audit-log windows, backup rotation, leaver deletions, disappearing messages.	3 Within 48 hours Confirm in writing what must be suspended today: retention pruning, backup recycling, chat auto-delete, device reissue. Convert the answers into the data map and custodian register.	4 After Feed the answers into the strategy memo (Guide 2 of this set) and DRD Section 2. Circulate the action list, not the meeting note: the note may be privileged, the actions must travel.
---	--	---	--

The V/A discipline matters because a fifty-question form returned by email produces fifty assumptions. An answer becomes "verified" only when a person with the relevant admin access has checked it.

03 Reading an answer

Answer	What it usually means
"IT will know"	Nobody in the room owns the fact. Book the IT lead before you leave.
"We keep everything"	Nobody has read the retention policy. Ask for the setting, not the belief.
"That laptop was reissued"	Unallocated space is being overwritten now. Quarantine today.
"Only on WhatsApp"	Personal devices, disappearing messages and control questions all just arrived.
"Our MSP has backups"	A third party holds evidence under a contract you have not read.

04 Checklist: what you leave the room with

- ☐ A dated answer set with V/A grading on every line
- ☐ A list of what is being suspended today, with named owners
- ☐ The IT lead's name and a follow-up slot within two working days
- ☐ Every leaver and reissued device identified
- ☐ Every messaging channel and its retention setting recorded
- ☐ Third parties who hold data, and the contract that reaches them
- ☐ Decision-log entries for anything not yet done, with a reason

Red flags

- ▶ Nobody from IT attends, or attends without admin access
- ▶ A hold "sent last week" that nobody can produce
- ▶ Chat retention still at the default 30 days
- ▶ A key custodian left within the last 12 months
- ▶ Answers offered from memory about backup schedules

WHEN TO INVOLVE THE LABORATORY

Bring an examiner to the meeting when a leaver, a wiped device, a deletion spree or a third-party host appears in the answers. A quarantine and log export that day costs an hour; the same evidence in month six may not exist.

Read the full guide

e-discovery.uk/library/the-first-edisclosure-meeting-50-questions-lawyers-should-ask
Free to read online or download. All CFL guides: e-discovery.uk/library

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

One-page guide 2 of 10

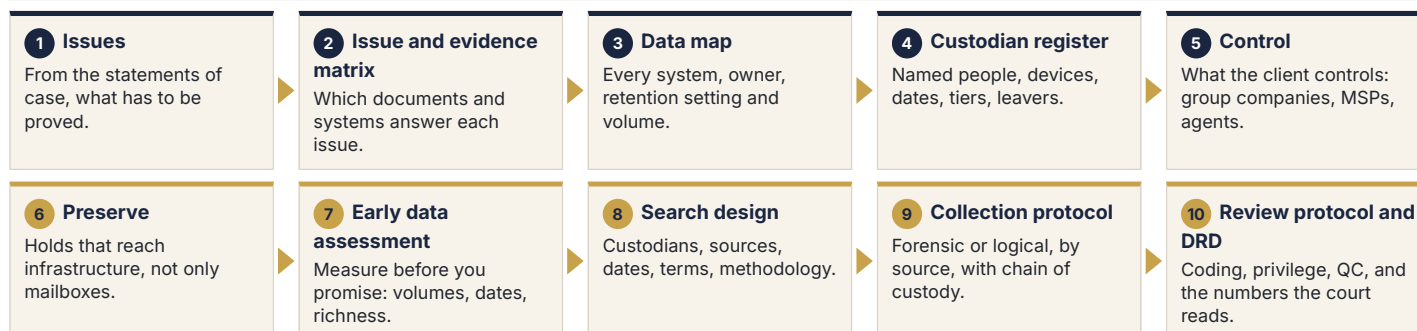
Condensed from the full CFL guide
(27 pages, e-discovery.uk library)

Ten building blocks, one memorandum, and a decision log that answers every later challenge.

THE HEADLINE POINT

Defensibility is built at the start and cannot be retrofitted. A strategy that runs issues, data map, custodians, control, preservation and early assessment in sequence, and records each decision as it is made, survives the specific-disclosure application, the costs argument and the certificate of compliance. One that starts at "search terms" does not.

01 Ten building blocks, in order, each producing a written output



Blocks 1 to 5 are answered mostly by lawyers and the client; 6 to 10 mostly by the provider and examiner. The order is not optional: a search designed before the data map exists is a search of an imagined estate. Each block writes a section of the memo below and one or more decision-log entries.

02 The strategy memorandum skeleton (Parts A to I plus decision log)

Part	Contents	Court-showable?
A to B	Issues, evidence matrix, what the case turns on documentarily	Yes
C to D	Data map and custodian register (current version, dated, signed off by IT)	Yes
E	Control analysis: group entities, MSPs, personal devices, contractual reach	Yes
F	Preservation taken: holds, suspensions, quarantines, dates, confirmations	Yes
G	EDA results and proportionality arithmetic	Yes
H	Search, collection and review protocols; DRD Section 2 feed	Yes
I	Tactical considerations: what to concede, where to press, cost exposure	No: kept separate
Annex	Decision log: every choice, the date, the reason, the alternative rejected	Yes

Keeping Part I physically separate means Parts A to H can be exhibited to a specific-disclosure application without a privilege fight.

03 Which track? Five-question calibration

Is deletion, theft or tampering alleged or suspected?	Forensic posture: image first, examine second, before anyone is confronted.
Is a rolling retention window about to close?	48-hour track: suspend and export today, then plan.
Are personal devices or chat apps in play?	BYOD track: consent, targeted collection, control analysis.
Does the client control the data it needs?	Control track: contracts, inspection rights, group companies.
Otherwise	Standard or light-touch track: scaled to value and volume. Tracks combine.

04 What the judge is asking, in every case

- ☐ Did you cooperate early and transparently on methodology?
- ☐ Was the search designed from the data, not from the pleadings alone?
- ☐ Are your estimates measured (volumes, hit counts, unit rates) or asserted?
- ☐ Did you preserve before you argued about proportionality?
- ☐ Can you show a decision log when a gap emerges?

Red flags

- ▶ No written strategy by the first CMC
- ▶ A data map the IT manager has never seen
- ▶ Search terms agreed before EDA ran
- ▶ Preservation notices that never reached the infrastructure team
- ▶ A memo with no version number or decision log

WHEN TO INVOLVE THE LABORATORY

Instruct the examiner at block 3 (data map) rather than block 9 (collection). Reading an estate accurately, tiering its backup platforms and pricing a targeted collection is an afternoon for a specialist and a hazard for anyone else.

Read the full guide

e-discovery.uk/library/how-to-build-a-defensible-edisclosure-strategy-at-the-start-of-a-case
Free to read online or download. All CFL guides: e-discovery.uk/library

Early Data Assessment Before Disclosure Costs Escalate

One-page guide 3 of 10
Condensed from the full CFL guide
(26 pages, e-discovery.uk library)

Measure the estate before you promise anything to the court, the client or the other side.

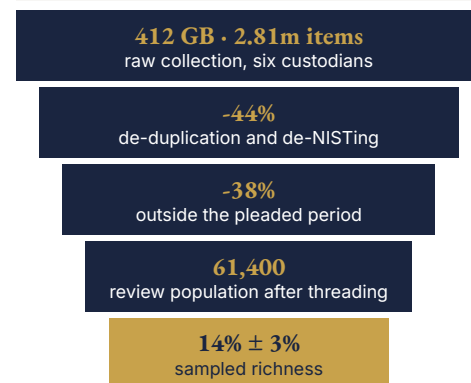
THE HEADLINE POINT

Every disclosure argument is eventually an argument about numbers: how many documents, from whom, over what period, at what richness and cost. Early data assessment produces those numbers in days, before models are chosen or terms agreed. The party holding measured figures wins the proportionality debate.

01 Seven measurements that convert guesswork into numbers

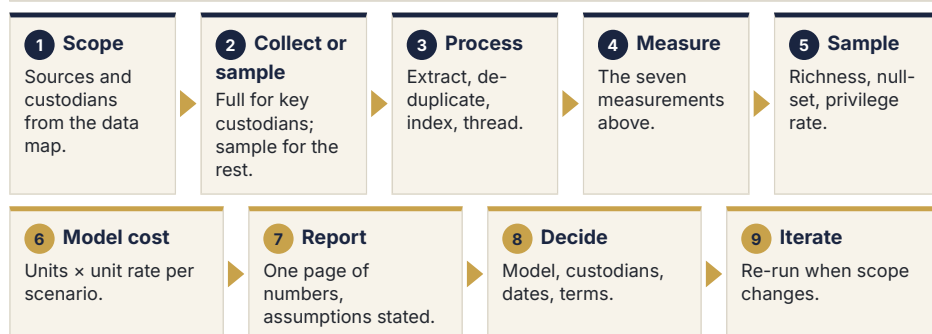
Volume GB and item counts per source and custodian after extraction.	Custodian spread Who actually holds the material; who is peripheral.	Dates Histogram of items by month against the pleaded period.	File types Email, office, chat, images, exotics that need special handling.
Duplication and noise Exact and near-duplicate rates; system mail; newsletters.	Communication patterns Who wrote to whom, when, on which channel.	Richness and privilege Sampled relevance rate and the share touching lawyers.	

02 Illustrative EDA funnel



Fictional series case study. The shape, not the numbers, is what repeats.

03 Nine-step workflow, and what each step feeds



04 Depth calibration

Small estate, no anomalies	Light touch: counts and dates only.
Search-based disclosure likely	Full EDA before the DRD Section 2 is drafted.
Merits still uncertain	EDA before filing: what the documents actually show.
Deletion or gaps suspected	EDA plus forensics: audit logs and backups in scope.
One narrow question	Targeted: a custodian, a window, a system.

05 Cost levers the numbers unlock

Lever	Typical effect
Date-range trim from EDA histogram	Often the single largest cut, defensible because measured
Custodian de-prioritisation	Peripheral custodians sampled, not reviewed in full
Threading and near-duplicate suppression	Review units fall; families and context preserved
Sampled richness per term	Six-figure hit terms renegotiated on arithmetic

06 Checklist

- ☐ EDA run before any search term is agreed
- ☐ Every number carries its assumptions and date
- ☐ Date histogram compared to the pleaded period
- ☐ Richness sampled with a stated confidence interval
- ☐ Results written into DRD Section 2 and Precedent H

Red flags

- ▶ Round numbers in a DRD estimate
- ▶ "We have about a million documents" from memory
- ▶ Hit counts quoted without richness
- ▶ A date histogram with a hole where a custodian should be
- ▶ EDA done after the CMC, to justify a position already taken

WHEN TO INVOLVE THE LABORATORY

Ask for an EDA when the estimate is due in the DRD and nobody has processed a byte, or when the date histogram shows a gap: an empty quarter for a key custodian is a preservation question, not a statistic.

Read the full guide

e-discovery.uk/library/early-data-assessment-before-disclosure-costs-escalate
Free to read online or download. All CFL guides: e-discovery.uk/library

THE HEADLINE POINT

The Disclosure Review Document is where PD 57AD turns cooperation into paper: Issues and Models in Section 1A, Model C requests in 1B, and twelve questions in Section 2 that only the client's IT, the provider and, where there are gaps, a forensic examiner can answer. The legal team edits; it should not invent. Paragraph 10 sets deadlines that ambush parties who leave the estimates to the last week.

01 Anatomy of the DRD, read in reverse order

Section 1A · Issues for Disclosure
One row per issue: agreed or not, each party's proposed Model, the court's decision, statement-of-case reference.

Section 1B · Model C requests
Party, issue, request, response, decision. Limited in number, focused, concise, not tactical.

Section 2 · Q1 to Q9
Hard copy; data sources (the form itself lists mobile, DMS, cloud, webmail, chat, backups, social media, third parties); proprietary software; custodians and date ranges; search proposals (keywords "for discussion only"); irretrievable documents (Q8); TAR with the 50,000-document justify-if-not threshold (Q9).

Section 2 · Q10 to Q12
Costs of agreed scope; each side's costs of the contested scope. The arithmetic the CMC decides on.

Start drafting from Section 2: the sources, custodians and estimates decide which Models are realistic in Section 1A. Only Models A and B on every issue? No DRD is needed at all.

02 Who feeds what

Client IT
Data map, retention settings, backup catalogues (Q2, Q3, Q8)

Custodian interviews
Names, devices, dates, channels (Q4)

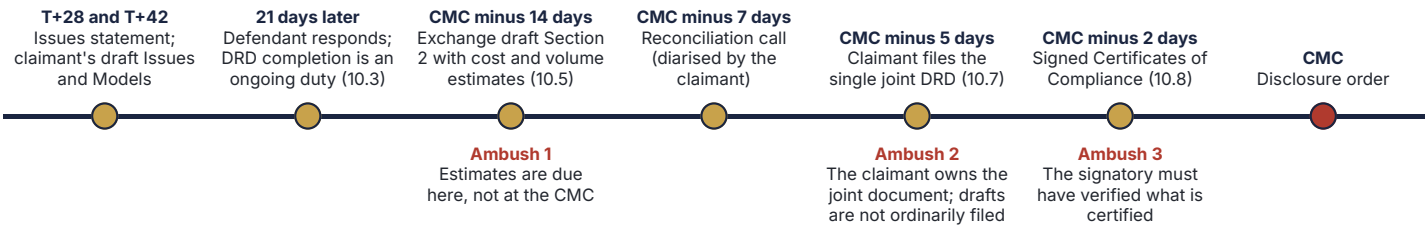
Provider hit counts
Per-term volumes and sampled richness (Q6, Q9)

Provider quotation
Unit rates, hosting, scenarios (Q10 to Q12)

Forensic examiner
What is irretrievable, and why, evidenced (Q8)

Legal team as editor
Issues, Models, requests, honesty of the whole

03 Paragraph 10 choreography: work backwards from the CMC



04 Question 8: the honest data-gap entry has four elements

1 What
The source, custodian and period that cannot be retrieved.

2 Why
The mechanism: leaver deletion, retention purge, device wipe, rotation.

3 Investigation
What was checked: audit logs, backups, counterpart copies, and by whom.

4 Mitigation
Where equivalent evidence is being pursued, and a para 10.3 commitment to update.

Facts, not characterisation. Candour on Q8 has repeatedly cost less than a gap discovered by the other side.

05 What a DRD-grade estimate contains (Q10 to Q12)

Measured volumes
Items per custodian and source after processing, with the date of the count.

Unit rates
Per-document review rate, hosting per month, processing per GB, from a quotation on file.

Stated assumptions
Threading, TAR, richness sample, privilege rate, what is excluded.

Scenario columns
Agreed scope, our contested scope, their contested scope: the arithmetic the court decides on.

Round numbers read as guesses. Every submission at the CMC should point to a number in the DRD.

Red flags

- ▶ Section 2 drafted by lawyers from memory of the IT estate
- ▶ Round-number estimates with no unit rate or volume behind them
- ▶ Q8 answered "none" without a forensic check
- ▶ Backups and chat platforms missing from Q2
- ▶ A certificate signed by someone who never saw the data map
- ▶ Cooperative over-sharing: methodology is transparent, strategy is privileged

WHEN TO INVOLVE THE LABORATORY

Q8 is the trigger. If any source is claimed to be irretrievable, the claim must rest on an examination of audit logs, backup catalogues and counterpart copies, evidenced so it can be defended at the CMC and, if needed, under CPR Part 35.

Read the full guide

e-discovery.uk/library/completing-the-disclosure-review-document-a-technical-and-legal-guide
Free to read online or download. All CFL guides: e-discovery.uk/library

How to Design Defensible Keyword Searches

Terms come from the data's own vocabulary; syntax is engineered per platform; every choice is tested and written down.

THE HEADLINE POINT

Most keyword lists are written like shopping lists: from memory, by people who were not in the kitchen. The people who wrote the documents called the product "Project Kestrel", the counterparty "PBL" and the problem "the wobble", and one of them typed "agreemnet" every time. A defensible list is harvested from the corpus, engineered against the platform's syntax, tested with hit counts and samples before agreement, and documented term by term.

01 The method: a list is built, not brainstormed

1 Harvest the vocabulary

Issues decomposed; the twenty key documents mined; ten-minute custodian interviews; early corpus sampling; the informal register (nicknames, codenames, typos, other languages).

2 Engineer the syntax

AND, OR, sparing NOT; wildcard expansion checked against the index; proximity connectors as the precision workhorse; platform dialect confirmed in writing.

3 Test before agreeing

Hit counts per term; sampled precision; null-set checks. Widen, narrow or replace on evidence, never on instinct.

4 Document the choices

A protocol file: per term, its origin, syntax rationale, test results, refinement history and version.

5 Declare the blind spots

What keywords cannot reach, and which tool covers it: OCR, analytics, TAR, structured queries.

02 The wildcard that ate the budget: a refinement cycle in numbers

212,000 hits

As agreed on a Friday, untested const* for "construction". Also matches constant, constable, constitute, constraint.

under 2%

Sampled relevance

A 200-document sample showed the term was almost entirely noise. Review estimate for this term alone: north of £300,000.

9,400 hits

Renegotiated construct* w/10 (defect* OR delay* OR variation*): the concept kept, the noise shed, the delta documented and recited in an amended order.

61%

Sampled relevance after refinement

The judge's observation: a two-hour test before agreement would have cost neither party anything.

03 Where terms come from

Issues layer

Parties, products, clauses, references, dates

skeleton

Key-document harvest

The words actually used in the 20 documents you already have

highest yield

Custodian interviews

"What did you call it?" Ten minutes each

irreplaceable

Corpus sampling

Frequency lists; words clustering beside known terms

the data proposes

Informal register

Typos, chat spellings, second languages

the candid layer

04 What keywords miss

Text that is not text

Scans and image-only PDFs are invisible until OCR runs. State the OCR posture or you are searching a partial corpus silently.

The unnamed wrongdoing

"As discussed", "the usual", "call me". Met by participant-and-date pulls and communication analytics.

Numbers and structured data

Spreadsheet values and metadata fields sit outside text indexes.

Language and encoding

Terms per language; diacritics; three spellings of one surname.

05 A null result is a routing instruction, not a finding

Nothing on a live issue

Harvest again; check the unindexed layer; run the participant-and-date pull as the safety net.

Too much noise

Proximity and intersection; narrow by window; let ranking triage.

Known documents not hit

Diagnose the term; check OCR; retrieve directly by custodian and date.

Opponent claims a null

Demand their variants, their OCR posture, their window pull and their method.

06 Checklist

☐ Harvest and interviews done before drafting; skeleton terms mapped issue by issue

☐ Platform dialect confirmed in writing and filed

☐ Every term hit-counted and sampled before exchange

☐ Wildcards expansion-checked; NOTs treated as scope decisions

☐ OCR posture stated; protocol file maintained with versions and deltas

WHEN TO INVOLVE THE LABORATORY

At design (harvest, dialect check, first hit analysis), at negotiation (refinement on evidence), at challenge (auditing an opponent's null) and at reporting, where search methodology becomes an issue under CPR Part 35.

Red flags

▶ Term lists exchanged without hit counts

▶ Six-figure hit terms accepted under a deadline

▶ Certified null results over an unstated OCR posture

▶ Chat searched with the email list; silent edits to an agreed list

Read the full guide

e-discovery.uk/library/how-to-design-defensible-keyword-searches

Free to read online or download. All CFL guides: e-discovery.uk/library

Should Backup Systems Be Searched for Disclosure?

Preservation is near-automatic; searching is a reasoned, evidenced choice. The technology has moved and the folklore has not.

THE HEADLINE POINT

Backups are routinely excluded as disproportionate, yet they are repeatedly the last copy on earth of a deleted mailbox, a departed custodian's files or a system as it stood before the dispute. Day one: stop the recycling and ask for the catalogue. Then decide the search question on facts about this estate's platform, this case's gaps and the only-remaining-source test, and take the position in the DRD on described evidence.

01 Two questions hiding inside one

Reflex Preserve?
Near-automatic once litigation is contemplated. Suspend recycling and overwrite for in-scope periods, export the catalogue, tell the other side what has been done. Cheap, immediate, rarely contested.

Reasoned Search?
A reasonableness and proportionality question resolved through the DRD. The answer has shifted with the technology: blanket "tape is disproportionate" claims now often misdescribe the estate.

02 Know what you actually have: four tiers, four cost realities

Modern platform
Disk or cloud backup with a searchable catalogue and item-level restore. A single mailbox from a nightly job in hours. **modest**

Structured tape library
Managed tape, live catalogue, compatible hardware. Slower and sequential, but indexed and priced per set. **estimable**

Legacy or orphaned media
Tapes outliving their software; formats from departed vendors; unlabelled boxes from an acquisition. **the real cost**

Ad hoc copies
USB rotations, replica NAS units, the old server in the cupboard. Cheap to image, often evidentially rich, rarely a legitimate exclusion. **cheap**

03 The decision framework: the only-remaining-source test

Is the backup the only copy left?	Departed custodian past leaver deletion; purged mailbox or chat; decommissioned or migrated system; a rolled-back interval. Search: restoration is the search.
Are versions over time the issue?	Backdating, document evolution, altered records. Search generationaly: month-ends, not nights.
Is the live estate intact and duplicative?	Custodians present, no deletion in issue. Preserve but do not search: say so in the DRD, with the catalogue described.
Is cost the objection?	Tier the platform, read the catalogue, run a sample restore. "Impossible" repeatedly becomes "Tuesday".
Who created the gap?	A party whose own deletion made the backup the only source argues inaccessibility from a weak seat.

04 Sweep the cheaper shelves first

1 Live retention layers
Deleted-item retention, litigation holds, version history.

2 Snapshots and replicas
Server and NAS snapshots; DR environments.

3 Archives and journaling
Indexed and cheap to search; often the best first stop for mail.

4 Counterpart copies
The same email in twelve other mailboxes; sync clients; local OSTs.

5 Backup generations
The deepest, slowest shelf. Restore to a controlled environment, never production; hash, log, deduplicate against the live corpus.

05 Alternative evidence paths

Evidence	Live + recycle	Snapshots	Backup generations	Archive	Counterpart	Deleted / recoverable
Departed custodian's mailbox	Retention window only	Sometimes	Y: the classic case	Y where journaling ran	Partially	Varies
Deleted files or folders	Recycle and versions: short reach	Y within retention	Y across generations	n/a	Possibly	Varies
Pre-dispute system state	n/a	Short range	Y: the deep reach	n/a	n/a	Generation-dependent

WHEN TO INVOLVE THE LABORATORY

At the hold (so the suspension instruction actually reaches the infrastructure team and any MSP), at tiering, for catalogue analysis and scoped estimates, and at any hearing where feasibility or cost is contested: a short CPR Part 35 statement decides close calls.

Red flags

- ▶ A preservation notice with no backup limb
- ▶ "The tapes would cost a fortune" from someone who has not named the platform
- ▶ Rotation still running weeks into the dispute
- ▶ Backups absent from the DRD entirely
- ▶ An "inaccessible archive" that turns out to have a search box

Read the full guide

e-discovery.uk/library/should-backup-systems-be-searched-for-disclosure
Free to read online or download. All CFL guides: e-discovery.uk/library

How to Draft an Electronic Disclosure Production Protocol

The agreement that decides every later argument, clause by clause, drafted with the engineers in the room.

THE HEADLINE POINT

Two parties producing without a protocol are two factories shipping parts without agreeing measurements. Every difference in platform defaults surfaces as a dispute at the worst time: the wrong format, stripped metadata, orphaned attachments, a load file that will not parse, a redaction that lifts off. The protocol is one negotiation held early, when positions are cheap because nothing has been built wrong yet.

01 Four clause families, and the disaster each one prevents

Formats

Native as the default, stated as such. A per-type schedule: email, office, spreadsheets (always native), presentations with notes, images with metadata, chat as structured export, databases as targeted extracts. Imaging only for stated cause; every conversion flagged; an exceptions mechanism for what the table missed.

Data

Metadata fields enumerated by name, not "standard fields". Families and parent-child links preserved in the load file. Threading and deduplication disclosed, with suppression reporting. Load-file specification precise to encoding, delimiter, date format and image-reference convention. Extracted text and OCR obligations stated.

Protections

Redaction standards: burn-in, sanitisation, no obfuscation, verification. Privilege schedules and partly privileged documents. Clawback in full: notice, non-use, return or certified deletion, no automatic waiver; a failed redaction treated as an inadvertent disclosure. Confidentiality tiers with a challenge route. UK GDPR posture stated once.

Operations

A mandatory sample exchange before the first tranche. Tranches with manifests (counts, ranges, hash totals). An intake and objection window. Correction mechanics with versioned control numbers and overlay files. An engineer-first dispute ladder. An amendment clause with version history.

02 Timing: agree it while every clause is still a setting, not a rebuild

1 DRD stage

Scope and Models negotiated. The protocol drafted alongside, from the data map, with both providers in the room.

2 Processing

Format, field and family choices are settings now. After this point they are rebuilds, priced accordingly.

3 Sample exchange

Fifty documents each way. Load files parsed, fields verified, images opened. The £500 rehearsal that catches the £50,000 incompatibility.

4 Tranches

Rolling production against the deadline, each with a manifest. Defects notified within the window and cured administratively.

03 The dispute ladder

1 · Engineer to engineer

Providers diagnose and agree a corrected specification, with authority to resolve.

days

2 · Solicitor to solicitor

Only what the engineers could not settle: allocation, scope, cost.

weeks

3 · The court

Reserved for genuine disagreement. Delimiter arguments should never reach a hearing list.

months

04 Reading the other side's template

Clause	What it may quietly allocate
Field list	Omitting file paths and container sources starves your provenance analysis
Threading	Inclusive-only production removes the intermediate messages your chronology needs
Correction costs	Allocated to the requesting party; you pay to fix their defects
Format default	Imaged PDF for spreadsheets: 4,100 pages instead of one working model
Clawback	Absent: a privileged escape has no machinery to invoke

05 Checklist

- ☐ Drafted from the data map; provider review on every technical clause
- ☐ Native default stated; spreadsheets native; per-type schedule complete
- ☐ Metadata fields named; families and links specified
- ☐ Load-file specification precise; sample exchange mandatory
- ☐ Redaction and clawback standards imported in full
- ☐ Tranches, manifests, intake windows and correction mechanics drafted
- ☐ Dispute ladder engineer-first; amendment and version history live

Red flags

- ▶ "Standard fields" or "usual format" anywhere in a draft
- ▶ A template offered for signature without platform review
- ▶ No sample-exchange clause on a multi-party matter
- ▶ Spreadsheets, chat or structured data missing from the schedule
- ▶ Correction costs allocated to the receiving party by default

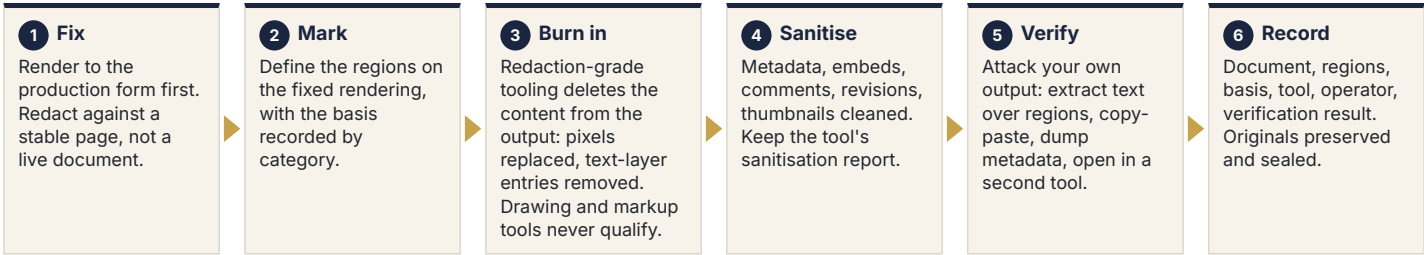
Digital Redaction That Cannot Be Reversed

Why black rectangles fail, how real redaction works, and how to verify it before it leaves the building.

THE HEADLINE POINT

On paper, a black marker destroys what it covers. A digital document is a rendering of underlying data, and drawing a rectangle changes the rendering while the text, metadata, embedded objects and revision history remain intact. Real redaction is a pipeline: burn in, sanitise every layer, verify adversarially, and keep the audit record that proves all three.

01 The pipeline: redaction is removal of data, not concealment of pixels



"If select-and-copy over the region yields text, it is not redacted." The one-line test that catches the most common failure in circulation, and the cheapest to prevent.

02 Where content hides

Visible rendering

the decoy

What the eye sees. A black rectangle changes this layer only.

Text layer

classic failure

The searchable text beneath. Extraction and copy-paste read straight through markup.

Metadata

core target

Title, author, comments, tracked changes. The settlement agreement whose title names the counterparty.

Embedded objects

whole documents

The spreadsheet behind the pasted chart; attachments inside PDFs; OLE objects.

Revision history

recoverable

The paragraph "removed" before production, still in the revision stream.

Image layers

obfuscation fails

EXIF and thumbnails preserving the pre-crop picture; blur and pixelation increasingly reversible.

03 The hard formats

SpreadsheetsCell values feed formulas; hidden sheets and pivot caches retain source data. Convert dependents to values, purge caches, audit hidden sheets, log the dependency check. Or image the sheet for cause.

Word-processing nativesRemove text, flatten revisions, sanitise metadata, re-save clean, and flag the edited native as a conversion.

Images and scansSolid-fill replacement, EXIF and thumbnail sanitisation, re-encode. Never blur or pixelate.

Audio, video and chatRe-encoded output with spans logged; chat redacted at export-generation by query where possible.

04 Receiving a redacted production

- Intake audit gains a redaction pass: bases stated, layers checked, not to harvest but to know what you hold.
- A failed redaction: stop, quarantine, notify. Mining it converts an opponent's error into your own conduct problem.
- Over-redaction is challenged through inspection machinery; the court can look behind the ink, you should not.

05 Plan across the estate, not the page

Where the passage also lives	Redactor's task	Recipient's legitimate route	Failure consequence
Duplicates	Propagate the same treatment to every copy	The produced duplicate	One missed copy leaks all
Thread instances	Redact every quoting hop	The produced thread	The unredacted quote, forty documents later
DMS versions and backups	Scope the version ladder; know what persists	Version production requests	The open earlier version
Unredacted originals	Preserve and seal under ring terms	Inspection machinery	n/a: the court's yardstick

Red flags

- Redactions that select, copy or extract
- The same passage open elsewhere in the production
- Spreadsheet redactions with live formulas nearby
- Blurred or pixelated text offered as redaction
- Productions with no stated redaction bases
- "We no longer have the unredacted version"

WHEN TO INVOLVE THE LABORATORY

At workflow design (tooling, sanitisation coverage, verification battery per format), at the outbound gate, on the receiving side for intake checks and over-redaction challenges, and as the neutral examining contested redactions against sealed originals under ring terms.

Read the full guide

e-discovery.uk/library/digital-redaction-that-cannot-be-reversed
Free to read online or download. All CFL guides: e-discovery.uk/library

Investigating Suspected Employee Data Theft

From first suspicion to springboard relief: won by the first fortnight's forensics, lost by the IT department's first afternoon.

THE HEADLINE POINT

Copying an employer's data is noisy: the platform logs the download, the endpoint logs the USB device, the browser logs the personal-cloud upload, the badge system logs the late visit. The trail's enemy is rarely the thief. It is the look-around that overwrites artefacts, the leaver process that deletes the account, and the confrontation held before anything was preserved.

01 First response: the freeze that happens before anyone investigates

1
Sequester devices

Laptop and phone held unpowered. No IT inspection, no reissue to a new starter.

➔

2
Hold accounts

Suspend and preserve: mailbox, cloud drive, chat, CRM. Litigation hold on; never delete through the leaver process.

➔

3
Export the perishables

Platform audit logs, sign-in records, DLP alerts, proxy logs. Rolling retention started before the suspicion did.

➔

4
Touch nothing as the user

No logging into the profile "for a look". Every such act overwrites timestamps and writes the contamination defence.

➔

5
Time the confrontation

Early confrontation risks the personal cloud being emptied; silence risks ongoing harm. Decide with advice, letter ready.

02 A choreography timeline

When	Event	Layer
Sunday 18:58	Badge entry to the office	Physical
19:12 to 20:31	CRM report exports across the whole desk	Platform
Same evening	Personal-cloud sync client mirrors 3,900 files	Endpoint
20:47	Badge exit	Physical
20:52	Resignation letter drafted	Endpoint
Monday	Resignation delivered; client calls by Wednesday	The tell

Fictional example. Exfiltration timed against resignation supplies intention.

03 The exfiltration artefact map: one story across independent layers

Evidence	Endpoint image	Platform audit logs	Mail system	Network / proxy	Physical layer	Counterpart estates
What was taken	Sync databases, LNK files, copies	Download and export lists	Attachment manifests	Transfer sizes	Print logs	The received copies
How it left	USB and upload artefacts	Sharing and egress events	Forwards and rules	Destinations	n/a	Arrival artefacts
When	Timestamps	Server clocks	Y	Y	Badges and CCTV	Receipt dates
Who (attribution)	User-context artefacts	Account, device, IP	Account	Source machine	The person	Possession
Cleanup attempts	Wiping tools, cleared history	Deletion events	Purged items	n/a	n/a	Personal-side deletions

Fallback in one line: exfiltration writes to at least three layers; preserve them all in week one, and when one is lost prove the transfer from the survivors, then reach the received copies through the ladder.

04 Escalation ladder, timed to the springboard clock

Letter

many end here

Preservation demanded across personal devices, accounts and media; undertakings sought: non-use, non-disclosure, delivery-up, imaging consent.

Orders

weeks

Delivery-up and imaging, commonly via an independent examiner reporting on relevant material only.

Injunction

the fortnight

Springboard and confidential-information relief, duration argued from the real life of the head start. Dies of delay.

New employer

in frame

Knowledge and receipt investigated; preservation obligations trigger the day they learn.

05 Lawful investigation and the innocent-explanation pass

☐ Purpose and scope documented under UK GDPR: the leaver's work estate, not their life; private material filtered by protocol

☐ Covert monitoring exceptional; Acas-consistent employment process running in parallel

☐ Privilege structured at instruction: litigation in contemplation, on day one

☐ Attribution joined to the person (badge, device, sign-in fingerprint), not assumed from the login

☐ Quantification by file-level manifest; artefacts tested against the defence's best case before anything is sworn

Red flags

▶ Mass activity in the resignation fortnight

▶ Personal sync clients on work endpoints; auto-forwarding to personal addresses

▶ Wiping tools or history-clearing dated to the exit

▶ IT "checks" already run, or leaver deletions running, despite live suspicion

WHEN TO INVOLVE THE LABORATORY

At the trigger, before anyone touches the estate: containment advice is a same-day call. Then through examination (artefact map, attribution, manifest, choreography) to CPR Part 35 evidence at injunction speed. The same machinery serves respondents: many artefacts have an innocent story that baselines reveal.

Read the full guide

e-discovery.uk/library/investigating-suspected-employee-data-theft

Free to read online or download. All CFL guides: e-discovery.uk/library

Preserving Evidence After a Cyber-Attack or Ransomware Incident

Recovering the business without destroying the case: one preserved estate serves the ICO, the insurer, the claimants and the court.

THE HEADLINE POINT

Recovery destroys evidence by default. The reimaged server loses the webshell; the restored share overwrites the encrypted files that identified the strain; the rotated credential closes the account whose sign-in history mapped the intrusion. Preserve in parallel, in the right order, with the mandate stated in writing, and every later question is answered from findings rather than recollection.

01 The first hours: preserve in parallel with recovery, in this order

1 Isolate, do not power off
Pull the network cable, not the plug. Memory holds tools, keys and sessions that disk never sees.

2 Capture volatile data
Memory, connections, processes from live compromised systems. Cannot be repeated.

3 Image before reimage
Patient-zero candidates, domain controllers and a sample of encrypted endpoints imaged as found.

4 Harvest the logs
Firewall, VPN, proxy, identity provider, EDR, cloud audit trails, backup and email-gateway logs. Hour one: retention does not pause.

5 Keep the incident log
Actions, times, actors, decisions from the first alert. Ransom notes and portals preserved.

02 The clocks

ICO
Notifiable personal-data breaches: without undue delay and within 72 hours of awareness; staged notification available **72 h**

Data subjects
High-risk breaches: without undue delay, scoped by what the evidence shows **no delay**

Sector regulators
FCA, NIS regime, listed-company disclosure, per client **per regime**

Sanctions and law enforcement
Ransom decisions under advice; NCSC and Action Fraud engagement **before payment**

PD 57AD
Litigation in contemplation: the incident estate is a disclosure event in waiting **hold now**

03 The intrusion evidence map: five phases, each provable or surmised

1 Entry
Phishing artefacts, exploited services, stuffed credentials, the abused vendor connection. Where supplier claims live.

2 Movement
Persistence, tool deployment, lateral authentication. The dwell-time question, with policy-period consequences.

3 Staging
Enumeration, searches, the multi-gigabyte archive in a temp folder: what was targeted.

4 Exfiltration
Egress volumes against baselines; transfers to attacker infrastructure. Sometimes provably negative.

5 Impact
Encryption sequence, deletion, log clearing, backup destruction: anti-forensics documented as evidence.

04 Layers fail differently

Layer	What it holds
Endpoint	Richest, most fragile. Recovery destroys it first.
Identity and platform	Survives reimaging; sits on rolling retention.
Network	Sees movement and egress independently of hosts. Attackers can clear a server's logs, not the firewall's memory.
Security tooling	EDR, gateway, backup-system records.
External	Threat intelligence, leak site, ransom portal, provider records.

05 The crowded bridge: insurers and IR firms

- Panel IR firms are optimised for containment, recovery and the claim. Evidential preservation is nobody's default mandate.
- State the mandate in the engagement, in writing: images retained and owned by the organisation, log exports delivered, actions documented.
- Structure privilege early and honestly: dual-purpose incident reports have fared badly.
- Send the preservation letter to the MSP or vendor on the suspected route today.

06 Checklist

- ☐ Isolation by disconnection; volatile captures first
- ☐ Representative systems imaged before rebuild, encrypted state included
- ☐ Log estate exported hour one; backup-system records preserved
- ☐ Ransom artefacts captured; advice taken on engagement
- ☐ IR engagement carries the written preservation mandate
- ☐ ICO position drafted from evidence, staged where needed

Red flags

- ▶ Recovery proceeding with no preservation inventory
- ▶ Compromised systems powered off "to be safe"
- ▶ Log retention shorter than plausible dwell time
- ▶ IR reports drafted for everyone and privileged for no one
- ▶ Notification scope asserted without exfiltration analysis

WHEN TO INVOLVE THE LABORATORY

In the first hours alongside the IR firm, to design and execute the preservation mandate while the estate still holds its story; through assessment, where provable non-exfiltration is hour-one work; and into supplier claims, coverage disputes and subject actions under CPR Part 35.

Read the full guide

e-discovery.uk/library/preserving-evidence-after-a-cyber-attack-or-ransomware-incident
Free to read online or download. All CFL guides: e-discovery.uk/library



Scan to save our contact details

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

How a specialist laboratory can assist: Computer Forensics Lab and its eDiscovery arm e-discovery.uk run each discipline in this digest as documented practice: data mapping and custodian registers, early data assessment, DRD estimates and Q8 investigations, search-protocol design and testing, backup tiering and targeted restoration, production-protocol drafting and sample exchanges, redaction engineering and verification, exit investigations to injunction standard, and incident-evidence preservation alongside insurer panels, with CPR Part 35 reporting where any of it becomes an issue.

© 2026 Computer Forensics Lab Ltd. General information, not legal advice. Full guides and references: e-discovery.uk/library.