



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Initial Disclosure: What Should Be Provided and What Should Be Preserved?

The Small Bundle and the Vast Universe

Initial Disclosure is deliberately small: the key documents relied on and needed to understand the case, served with the pleadings. Preservation is deliberately vast: everything potentially relevant, held intact until the case ends. The two obligations run on entirely different scales, and confusing them produces both classic failures: parties who provide too much, and parties who preserve too little. This guide explains each obligation, the relationship between them, and how the small bundle must be drawn defensibly from the wider electronic evidence universe.

⌚ Estimated reading time: 28 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**, works both scales of this guide daily: preservation and identification across whole estates, logged as the chain of custody opens, and the disciplined assembly of small, high-stakes bundles (Initial Disclosure, injunction exhibits, regulatory responses) from those preserved sources with natives, metadata and provenance intact. Our examiners also produce CPR Part 35 and CrimPR Part 19 compliant expert reports where documents in the small bundle are themselves challenged.

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

- 01 Executive summary
- 02 The problem in plain English: two circles, two scales
- 03 The legal framework
- 04 What should be provided: the Initial Disclosure bundle
- 05 What should be preserved: the whole universe
- 06 The relationship: how the bundle and the universe interact
- 07 Assembling Initial Disclosure defensibly
- 08 Reading an opponent's Initial Disclosure
- 09 Worked examples
- 10 Common mistakes and technical limitations
- 11 Questions to ask · Suggested wording
- 12 Checklist and red flags · When to involve a digital forensic expert
- 13 Frequently asked questions
- 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

Executive summary

THE HEADLINE ANSWER: PROVIDE LITTLE, PRESERVE EVERYTHING

Under PD 57AD, Initial Disclosure is served with each statement of case and contains only the key documents on which the party relies and the key documents necessary for the other parties to understand the claim or defence they must meet, without any search beyond what is reasonable, and capped (unless the parties agree or the court orders otherwise) at the larger of 1,000 pages or 200 documents.

Preservation, by contrast, attaches from the moment proceedings are contemplated and covers the entire universe of potentially relevant documents, in every source and format, whether helpful, harmful or unread, until the proceedings end. Provide a small, deliberate, well-evidenced bundle; preserve everything from which that bundle, and every later disclosure, might be drawn. Parties fail in both directions: over-providing (dumping documents into Initial Disclosure) and, far more dangerously, under-preserving (treating the small bundle as the whole obligation).

- **The two duties differ in every dimension.** Purpose, trigger, scope, effort, timing and the consequence of error: §6's comparison table sets them side by side, because the single most common client misunderstanding is that serving Initial Disclosure means "disclosure is done".
- **The bundle comes from the universe.** Even sixty documents must be drawn defensibly from preserved sources: native versions, metadata intact, provenance recorded, because relied-on documents are precisely the ones opponents challenge, and a key contract served as a metadata-stripped scan is an authenticity argument waiting to happen.
- **Initial Disclosure is strategic signalling.** What you provide frames the court's first view of the merits; what you omit, and what your opponent omits, is early intelligence about custodians, sources and confidence. §8 covers reading the other side's bundle forensically.
- **Preservation neither starts nor ends with the bundle.** It starts earlier (contemplation) and ends later (conclusion of proceedings), and nothing about serving Initial Disclosure relaxes a single hold, timer suspension or third-party notice.
- **Known adverse documents are a separate track.** Initial Disclosure does not require them; the freestanding duty to disclose them is discharged later, within the Extended Disclosure timetable (or the fallback timetable where none is ordered). Confusing the two produces both false comfort and false alarm.

The problem in plain English: two circles, two scales

Picture two circles. The inner circle is tiny: the documents served with the pleading, perhaps forty to two hundred items, chosen by the legal team because they carry the case or explain it. The outer circle is enormous: every mailbox, chat thread, drive, phone, backup and third-party holding that could contain something relevant to the issues, running to hundreds of gigabytes in an ordinary commercial dispute. Initial Disclosure is the inner circle. Preservation is the outer one. Almost every early-stage failure in disclosure practice is a confusion of the two:

CONFUSING OUTWARD (OVER-PROVIDING)	CONFUSING INWARD (UNDER-PRESERVING)
Treating Initial Disclosure as a mini standard disclosure: hundreds of marginal documents dumped with the pleading "to be safe", breaching the cap's spirit if not its letter, burying the key documents, educating the opponent for free, and signalling a team that has not decided what its case is	Treating the provided bundle as the obligation discharged: the client hears "disclosure served", relaxes, and the timers resume, the leaver's laptop is reissued, the WhatsApp thread is cleared, eighteen months before Extended Disclosure asks where it all went
Cost: tactical and presentational, usually recoverable	Cost: spoliation exposure, adverse inference, certificate jeopardy, sometimes irrecoverable

The correction is one sentence, repeated to the client until it sticks: **what we provide now is a fraction of what we must keep, and keeping it is the harder, longer duty**. The rest of this guide is the machinery behind that sentence.

The legal framework

- **Initial Disclosure (PD 57AD paragraph 5):** with its statement of case, each party serves an Initial Disclosure List of Documents and copies of (a) the key documents on which it relies (expressly or otherwise) in support of the claims or defences advanced, and (b) the key documents that are necessary to enable the other parties to understand the claim or defence they have to meet. No search is required beyond what is reasonable; documents already in the other party's possession need not be re-provided; and the obligation does not apply where it would (by the larger of the measures) exceed 1,000 pages or 200 documents, or where the parties agree in writing to dispense with it, or the court orders otherwise. Documents are provided electronically unless otherwise agreed, and the list identifies what is provided; no disclosure certificate is required at this stage, though the honesty duties apply in full.
- **Preservation (paragraphs 3 and 4):** the duty to take reasonable steps to preserve documents in a party's control that may be relevant to any issue in the proceedings attaches once proceedings are contemplated. It includes an obligation to suspend document deletion and destruction processes, to notify relevant employees and former employees, to notify third parties who may hold documents on the party's behalf, and to obtain written confirmation that steps have been taken. Legal representatives owe parallel personal duties. The duty runs until the proceedings conclude.
- **Known adverse documents (paragraphs 3 and 9):** a separate, continuing duty, not an Initial Disclosure requirement: known adverse documents are disclosed with Extended Disclosure, or within the timetable the PD sets where no Extended Disclosure is ordered on the relevant issue.
- **Outside the Business and Property Courts:** CPR 31 has no Initial Disclosure stage; the functional analogues are pre-action protocol disclosure of key documents and the strategic exhibiting of documents to statements of case. The preservation logic, however, is universal: duties arise when litigation is reasonably contemplated, and the two-scales discipline applies wherever you litigate. Scotland, Northern Ireland, arbitration and criminal proceedings run their own regimes, as flagged throughout this series.

What should be provided: the Initial Disclosure bundle

Selection is an exercise in discipline, run issue by issue against the draft pleading:

- **Limb one, relied on:** the documents the pleading stands on, expressly or by necessary implication: the contract and its operative variations, the pivotal correspondence, the notice served, the invoice unpaid, the report relied on. If a paragraph of the pleading would be challenged with "show me", the answer belongs in the bundle.
- **Limb two, necessary to understand:** the documents the other side genuinely needs to comprehend the case it must meet, which is a comprehension test, not a completeness test: the framework agreement referred to throughout, the key chain that explains the pleaded chronology. Resist the drift from "necessary to understand" to "helpful context"; the second phrase has no limit.
- **What stays out:** the merely supportive mass (Extended Disclosure's job), the adverse material (a different duty on a different clock), privileged documents (not disclosable at all, and relying on a document waives carefully, so check before including anything advice-adjacent), and padding of every kind: the cap is a ceiling, not a target, and a lean bundle of genuinely key documents is both compliant and rhetorically stronger.
- **Volume reality:** most well-run commercial pleadings produce bundles of 30 to 120 documents. If the genuinely key documents exceed the cap, the PD's own machinery answers (the obligation yields, and the position is explained), but interrogate the count first: a list over the cap usually contains Extended Disclosure material wearing an Initial Disclosure badge.
- **The list matters:** a clean, numbered Initial Disclosure List with stable document IDs, dates, descriptions and (internally) source references starts the matter's document-control discipline; the numbering you choose now will be cited at trial, so choose a scheme that scales.

What should be preserved: the whole universe

Preservation scope is set by potential relevance to the issues, not by what anyone intends to provide, rely on or even read. In practice that means the full modern estate mapped in our companion guide *Finding the Evidence*:

- **Communications:** corporate email and archives, chat and collaboration platforms (Teams, Slack), messaging apps on work and (where used for work) personal devices, shared and delegated mailboxes, with disappearing-message settings disabled in writing.
- **Endpoints and media:** issued laptops and phones, the leaver-device pipeline frozen, the storeroom shelf and the drawer of old handsets, removable media where it features.
- **Repositories and systems:** file shares, cloud drives and sites, the SaaS estate (found through accounts-payable and SSO cross-checks), structured business systems preserved through holds, snapshots or report baselines with their audit trails.
- **Backups and logs:** rotation paused for in-scope systems; platform audit logs (short retention windows) exported or held; CCTV and access records where physical events matter.
- **Third-party holdings:** MSPs, hosts, processors and former providers notified in writing; the client's own written preservation confirmation obtained and filed.

Two disciplines keep the outer circle honest. **Preserve does not mean collect:** most of the universe is held in place under holds and suspensions, with collection following later, source by source, as scope decisions are made; the preserve-only tier exists precisely so breadth of preservation never becomes breadth of processing. And **preservation is evidenced, not assumed:** the hold register, suspension confirmations and notices are the record that the outer circle actually existed, which is what an opponent's spoliation theory eventually tests.

The relationship: how the bundle and the universe interact

	INITIAL DISCLOSURE (PROVIDE)	PRESERVATION (KEEP)
Purpose	Frame the case; let the other side understand what it must meet	Keep every later option (and duty) performable: Extended Disclosure, adverse documents, forensic questions
Trigger	Service of each statement of case	Contemplation of proceedings, before any pleading exists
Scope	Key documents only; capped; no search beyond reasonable	Everything potentially relevant, in every source, helpful or harmful
Effort	Selection and curation by the legal team	Systems work: holds, suspensions, freezes, notices, registers
Duration	A moment: served and done (updated only via the pleading it accompanies)	Continuous until the proceedings end
Error mode	Over-provision: tactical cost, cap breach, waiver risk	Under-preservation: spoliation, inference, sanction

Beyond the contrast, four live connections:

- **The bundle is drawn from the universe, and must be traceable to it.** Every provided document should have a provenance answer: which preserved source, collected when, by whom, hash-verifiable against the original. The relied-on documents are the ones most likely to be challenged, so they justify the most careful handling, not the least.
- **The bundle predicts the universe's future.** Your selections signal which custodians, channels and periods matter; opponents read them exactly that way when negotiating the DRD (and so should you, §8). Choose knowing that each document is also a disclosure about your sources.
- **The bundle does not shrink the universe.** Nothing provided, and nothing about serving it, narrows preservation by one byte; scope reductions come later, openly, through the DRD's staged and preserve-only mechanics with reasons recorded.
- **The universe rescues the bundle.** When a provided document's authenticity, date or completeness is challenged, the answer lives in the preserved source: the native file, the mailbox copy, the server metadata, the forensic image. A party that preserved properly answers such challenges in days; one that kept only the courtesy copies litigates them for months.

Assembling Initial Disclosure defensibly

- **Preserve first, select second.** The day-one machinery (hold, suspensions, notices) runs before bundle assembly starts, so selection happens inside a protected universe rather than a shrinking one.
- **Collect the candidates properly.** Even a small bundle is collected, not gathered: exports from preserved sources under a simple logged protocol, natives retained with metadata intact, hashes recorded. The client forwarding "the important emails" from their live mailbox is how relied-on documents acquire modified dates and missing attachments.
- **Keep families together.** An email relied on travels with its attachments; a spreadsheet relied on is preserved native even if a PDF rendering is served for convenience; a chat excerpt is captured with enough thread to be honest, from a properly extracted source rather than a screenshot where it matters.
- **Run the privilege and waiver check.** Anything advice-adjacent gets a deliberate decision with the waiver consequences considered; reliance is a choice, not an accident.
- **Build the internal provenance schedule.** A one-line entry per document (source, custodian, collection date, hash reference) that is never served but answers every later challenge in minutes; it is the small-scale version of the collection logging that Extended Disclosure will require anyway, and starting the discipline here means one system, not two.
- **Serve electronically, sensibly:** text-searchable copies, stable numbering, the list reconciling exactly to what is provided, and natives available on request for anything whose formatting or formulas carry meaning.

Reading an opponent's Initial Disclosure

The other side's bundle is early, free intelligence, and it repays structured reading:

- **Map it to their pleading.** Pleaded allegations with no supporting document in the bundle are either held back (possible) or thin (more often); both readings inform the Defence or Reply and the first requests.
- **Read the sources between the lines.** Whose mailboxes do the provided emails come from? Which channels appear (and which obviously used ones do not)? What date ranges cluster? This is a first draft of their custodian and source landscape for DRD purposes.
- **Check the physics.** Scans of prints where natives must exist, screenshots of chats, missing attachments referenced on the face of provided emails, date formats that suggest re-creation: each is a question to ask now, politely and in writing, and a forensic flag if the answers wobble.
- **Log the gaps for later.** The absent variation everyone knows exists, the unexplained silence over the critical fortnight: today's observation is the DRD negotiation's exhibit and, if it hardens, the specific-disclosure application's foundation.
- **Ask early where it matters:** a short letter noting apparent gaps or requesting natives is proportionate at this stage and builds the cooperation record either way.

Worked examples

EXAMPLE 1 · THE BUNDLE WITHOUT A UNIVERSE

A claimant contractor served a tidy Initial Disclosure of 44 documents with its Particulars and considered disclosure handled. No hold was issued; the site manager left in month three and his phone, dense with the WhatsApp threads that ran the project, was factory-reset on reissue; the Teams retention timer ran on. At Extended Disclosure the gaps were unmissable (the defendant's own copies of chats had no counterparts), the correspondence about preservation dates was excruciating, and the trial judge's adverse inferences on the chronology issues cost far more than the claim's disputed variations. The 44 documents were fine; the missing universe decided the case.

EXAMPLE 2 · THE DUMP

A defendant served 1,800 pages with its Defence "in the interests of transparency": chains in quintuplicate, board packs, marginalia. The key documents drowned; the claimant's team mined the excess for admissions and source intelligence; and at the CMC the court observed that a party unable to identify its own key documents at the pleading stage inspired limited confidence in its approach to Extended Disclosure. Over-provision bought no credit and surrendered the framing advantage that a lean, deliberate bundle exists to capture.

EXAMPLE 3 · THE RELIED-ON DOCUMENT THAT COULD NOT STAND UP

A lender's case rested on a signed facility letter, served in Initial Disclosure as a scanned PDF. The borrower denied signing that version. The scan's provenance was a folder on a departed employee's desktop, collected by drag-and-drop; no native, no mailbox transmission copy, no metadata. Months of authenticity skirmishing followed until a forensic examination of the preserved mail server located the execution-version attachment with intact transmission metadata, resolving in the lender's favour what proper initial handling (native-first collection with a provenance line) would have foreclosed in a day.

Common mistakes and technical limitations

Common mistakes

- **"Disclosure done."** The client (or the fee-earner) equating service of Initial Disclosure with discharge of disclosure obligations, and preservation quietly decaying from that day.
- **Bundle assembly by forwarding.** Key documents emailed around, re-saved, printed and re-scanned, shedding metadata at every step, for the precise documents most likely to be challenged.
- **Padding toward the cap.** Treating 200 documents as an allowance to spend rather than a ceiling to stay far beneath.
- **Accidental waiver.** Advice-adjacent material included without a deliberate privilege decision.
- **The orphaned attachment.** Emails provided without the attachments they rely on, or attachments without their transmitting emails, inviting completeness questions on day one.
- **No provenance schedule.** Six months later, nobody can say where the relied-on spreadsheet came from, and the question has become hostile.
- **Ignoring the opponent's bundle.** Free intelligence unread, gaps unlogged, natives unrequested, and the DRD negotiated without the map their own selections provided.
- **Confusing the adverse-documents clock.** Either panic-including harmful material in Initial Disclosure (not required) or forgetting the separate duty exists at all (dangerous).

Technical limitations

- **Small bundles still need real handling.** Hash verification, native retention and logging scale down gracefully; skipping them because the volume is small is a choice, not a constraint.
- **Renderings lose content.** PDFs of spreadsheets drop formulas and hidden sheets; prints of emails drop headers; screenshots of chats drop everything forensic. Serve conveniences where sensible, but preserve and be ready to produce the natives.
- **Chat resists excerpting.** A message reads differently with its surrounding thread; excerpts served for concision should come from complete, properly extracted preservation copies so the fuller context is producible when fairness requires it.
- **Preservation cannot be retrofitted to the bundle's standards.** If the universe was not held from contemplation, no quality of bundle assembly repairs it; the two obligations fail independently.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- For each key allegation we plead: which document proves it, where does the original live, and who can retrieve it without touching anything else?
- Do you understand that what we serve now is a fraction of what must be kept, and that every hold and suspension stays in force after service?
- Is anything we propose to rely on a copy, a print or a forward rather than the source version? Where is the source?
- Does anything in the candidate bundle involve legal advice or lawyers, so we can make the waiver decision deliberately?

Ask your opponent

- Please provide the native versions (with metadata) of documents [x, y, z] provided in your Initial Disclosure.
- Document [n] refers to an attachment / an earlier chain not provided; please supply it or explain its omission.
- Please confirm the preservation steps taken and their dates, including in respect of [the departed individual / the messaging channel evident from your documents].
- Your pleading at paragraph [x] alleges [y]; no supporting document appears in Initial Disclosure. Please confirm whether such documents exist.

Ask an eDiscovery / forensic provider

- Can you support a fast, logged collection of a small candidate set from preserved sources, natives and hashes intact, inside a pleading deadline?
- What does your provenance record look like per document, and can it later scale into the full collection logging for Extended Disclosure?
- If a relied-on document is challenged, what examination and CPR Part 35 support can you provide, and from what preserved sources would you work?

SUGGESTED WORDING · CLIENT LETTER PARAGRAPH ON THE TWO OBLIGATIONS

"Two separate obligations apply and it is vital not to confuse them. First, with our statement of case we will serve a small set of key documents (Initial Disclosure). Second, and entirely separately, the company must continue to preserve every document that could be relevant to any issue in the dispute, in every location and format, whether or not it is helpful and whether or not it is ever served: this duty began when the dispute was first contemplated and continues until the proceedings end. Serving Initial Disclosure changes nothing about preservation: all holds, suspended deletion settings, retained devices and third-party notices remain in force, and no system, account or device relevant to the dispute may be altered, cleared or disposed of without our prior written agreement."

SUGGESTED WORDING · INITIAL DISCLOSURE COVER PARAGRAPH

"We enclose the [Claimant]'s Initial Disclosure List of Documents and electronic copies of the documents listed, served pursuant to paragraph 5 of PD 57AD with the [Particulars of Claim]. The documents comprise the key documents relied on and the key documents necessary to enable your client to understand the claim it has to meet; they are provided without prejudice to Extended Disclosure, which our client anticipates requesting, and no inference should be drawn as to the existence or otherwise of further documents from their selection. Native versions of any listed document are available on request. Copies are text-searchable and numbered [ID.0001] onwards; we propose the parties adopt a common numbering protocol for the proceedings and will write separately with a proposal."

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

The provide-and-preserve checklist

- ☐ Preservation machinery live and evidenced before bundle work starts: hold, suspensions, leaver freeze, third-party notices, written confirmation
- ☐ Client told, in writing, that service changes nothing about preservation
- ☐ Bundle selected issue by issue against the pleading: relied on, and necessary to understand, nothing else
- ☐ Every candidate traced to a preserved source; collected under a logged protocol; natives and hashes retained
- ☐ Families intact: attachments with emails, threads with excerpts, natives behind renderings
- ☐ Privilege and waiver check run on anything advice-adjacent
- ☐ Internal provenance schedule completed, one line per document
- ☐ List reconciles exactly to documents served; numbering scheme chosen to scale; served text-searchable and electronic
- ☐ Cap respected as a ceiling; any over-cap position analysed and explained, not defaulted into
- ☐ Opponent's bundle read forensically: pleading map, source signals, physics check, gap log, natives requested

Red flags

- Anyone saying "disclosure is done" in the same month as service of a pleading.
- Key documents arriving by forward from a live mailbox rather than by logged collection.
- A relied-on document that exists only as a scan, screenshot or print.
- An opponent's bundle of scans where natives must exist, or with attachments referenced but absent.
- A provided chat excerpt whose surrounding thread nobody has preserved.
- Timers, devices or accounts "released" after service because the bundle went out.
- An Initial Disclosure list flirting with the cap in a case whose pleading cites a dozen documents.

When to involve a digital forensic expert

Three moments in this guide's territory call for the laboratory. First, at preservation, where the universe includes volatile or suspect sources (leaver devices, central handsets, systems with deletion questions) needing forensic acquisition so the outer circle is real. Second, at assembly, where a document that will carry weight exists only in degraded form: examination of preserved sources (mail servers, file systems, backups) can locate the native, the transmission copy and the metadata that make it defensible before it is served. Third, on challenge, where an opponent disputes (or you dispute) a provided document's authenticity, date or integrity: artefact-level examination and a CPR Part 35 report resolve what correspondence cannot. The escalation discipline is in the companion guides *eDisclosure or Digital Forensics?* and *How to Build a Defensible eDisclosure Strategy*.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is Initial Disclosure "our disclosure done"?

No. It is the first, smallest instalment: the key documents relied on and needed to understand the case, served with the pleading. The preservation duty (everything potentially relevant, until the case ends), the known-adverse-documents duty and Extended Disclosure all continue on their own tracks, untouched by service. The most expensive misunderstanding in this area is a client who relaxes preservation because a bundle went out.

Do we have to include documents that harm our case?

Not in Initial Disclosure: its two limbs are documents relied on and documents necessary to understand the case, and it is not the vehicle for adverse material. But the separate duty to disclose known adverse documents is real, personal and continuing; it is discharged with Extended Disclosure (or within the PD's fallback timetable where none is ordered on the issue). Educate the client on both clocks so neither false comfort nor panic sets in.

What if our key documents exceed 1,000 pages or 200 documents?

First interrogate the count: bundles over the cap usually contain Extended Disclosure material mislabelled as key. If the genuinely key set still exceeds the cap, the PD's own structure responds: the obligation does not apply in that form, the parties can agree a sensible approach, and the position is explained to the court; what is not acceptable is silently serving a partial set that purports to be complete.

Can we agree to dispense with Initial Disclosure?

Yes, in writing, and it is sometimes sensible (key material fully exchanged pre-action, or an imminent limitation deadline making assembly impractical). Record the agreement, and remember dispensation touches only the providing obligation: preservation and the adverse-documents duty are wholly unaffected.

What format should we serve in, and must we give natives?

Electronic and text-searchable by default, with a clean reconciling list and stable numbering. Serve renderings for convenience where they are faithful, keep natives preserved regardless, and provide natives on request wherever formatting, formulas or metadata carry meaning; offering them unprompted for the load-bearing documents is cheap credibility.

Does the preservation duty ever relax as the case narrows?

Scope evolves openly, not by decay: preserve-only tiers, staged sources and reasoned exclusions are recorded in the DRD as the issues crystallise, and material genuinely outside any issue can eventually be released from hold with a documented decision. What never happens defensibly is quiet relaxation: a timer resumed or a device reissued without a recorded, reasoned decision is tomorrow's spoliation correspondence.

§ 1 4 · REFERENCE

Glossary

Cap

Initial Disclosure's ceiling: the larger of 1,000 pages or 200 documents, absent agreement or order.

Dispensation

The parties' written agreement (or the court's order) that Initial Disclosure need not be given.

Family

A document and its attachments or embedded items, kept and served together.

Initial Disclosure List

The numbered list identifying the documents provided with a statement of case.

Known adverse document

A document a party knows of that damages its case; disclosed on the Extended Disclosure timetable, not in Initial Disclosure.

Native version

The document in its original electronic format with metadata intact, as against prints, scans and renderings.

Preservation universe

Everything potentially relevant to any issue, in every source, held from contemplation to conclusion.

Provenance schedule

The internal one-line-per-document record of source, custodian, collection date and hash.

Relied on

Initial Disclosure limb one: documents the pleading depends on, expressly or otherwise.

Necessary to understand

Limb two: documents the other side needs to comprehend the case it must meet.

Spoilation

Loss or destruction of evidence that should have been preserved, and the inferences and sanctions that follow.

Waiver

Loss of privilege through deployment; the risk checked before anything advice-adjacent enters the bundle.

Sources and authoritative references

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

- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (holds, suspensions and logged, hash-verified collection from preserved sources): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, EDRM Phase 01 · Identification (mapping the universe the bundle is drawn from) and the practice's method statement ("Bring us in early. Defensibility is built, not retrofitted"): e-discovery.uk/edrm/identification · e-discovery.uk
- e-discovery.uk, Knowledge Centre practice notes: e-discovery.uk/knowledge
- cflab.uk, digital forensics services (locating natives, transmission copies and metadata in preserved sources; authenticity examination and CPR Part 35 reporting when provided documents are challenged): cflab.uk/digital-forensics-services
- cflab.uk, guides for lawyers, including document metadata and the perils of prints, scans and screenshots: cflab.uk/guides
- Practice Direction 57AD, paragraphs 3 to 5 and 9 (duties, preservation, Initial Disclosure, known adverse documents), with the DRD forms: justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd-57ad)
- CPR Part 31 and PD 31B (the position outside the B&PCs) and the Pre-Action Protocols (key-document exchange pre-action): justice.gov.uk, [PD 31B](https://justice.gov.uk/pd-31b) · [justice.gov.uk, Protocols](https://justice.gov.uk/protocols)
- CPR Part 35 (experts): justice.gov.uk, [Part 35](https://justice.gov.uk/part-35)
- ICO, UK GDPR guidance: ico.org.uk · Data Protection Act 2018: legislation.gov.uk/ukpga/2018/12

DISCLAIMER

This publication provides general information about Initial Disclosure and preservation practice in the United Kingdom as at August 2026. The worked examples are fictional illustrations. Paragraph references are indicative and the Practice Direction and its forms are amended from time to time; always check the current text. This guide is not legal advice, 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. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

The two scales of this guide are the two halves of our practice. On the universe side, **e-discovery.uk** makes preservation real on the day it is owed: in-platform holds and timer suspensions, leaver devices acquired under chain of custody, third-party notices supported, and the hold register that later proves the outer circle existed. On the bundle side, we run fast, logged collections of small candidate sets inside pleading deadlines, natives and hashes intact, with a provenance schedule that scales straight into Extended Disclosure's collection logging, and where a load-bearing document exists only as a scan or a forward, the laboratory locates the native and its metadata in the preserved sources before service rather than after challenge. When a provided document is disputed, our examiners resolve authenticity, dating and integrity at artefact level and report under CPR Part 35 / CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine, including a fixed-fee Initial Disclosure collection package for pleading-stage deadlines.



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

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