COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Electronic Disclosure Explained

A Practical Guide for UK Lawyers

The complete lifecycle of electronically stored information in litigation, from identification and preservation through collection, processing, review, production and eventual disposal, written for solicitors, barristers, litigation partners, associates, paralegals, in-house counsel, disclosure lawyers, investigators and litigation-support professionals.

⏱ Estimated reading time: 35 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. Our examiners produce CPR Part 35 and CrimPR Part 19 compliant expert reports for solicitors, barristers, in-house counsel and private clients, and give evidence in the Crown Court, County Court, High Court and employment tribunals.

Through our dedicated e-discovery practice at **e-discovery.uk**, we support law firms and in-house teams across the full disclosure lifecycle: defensible preservation and collection, forensically sound processing, hosted review, technology-assisted review, and production in court-compliant formats, with continuity of evidence maintained from identification to production.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | CPR PART 35 EXPERT REPORTS | CRIMPR PART 19 EXPERT EVIDENCE | PD 57AD / DRD EXPERIENCE | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

Electronic disclosure (eDisclosure) is the process by which parties to litigation identify, preserve, collect, process, review and produce **electronically stored information (ESI)**, emails, chat messages, documents, spreadsheets, databases, mobile data, cloud accounts and their metadata, in a manner that satisfies the parties' disclosure duties and withstands challenge.

It is emphatically not "exchanging documents, but on a computer". Electronic material differs from paper in volume, volatility, duplication, hidden content and metadata, and the procedural rules treat it differently as a result. A lawyer who runs an eDisclosure exercise like a paper exercise will over-collect, over-spend, miss responsive material, destroy metadata, and hand the opponent a platform for criticism at the case management conference.

SEVEN POINTS TO HOLD ONTO

- **The duty to preserve arises early**, as soon as litigation is contemplated, not when proceedings are issued. Written legal-hold notices, suspension of auto-deletion and preservation of departing employees' data are expected of the parties and their solicitors.
- **Two civil regimes coexist in England & Wales.** Practice Direction 57AD governs most Business and Property Courts claims (Initial Disclosure, Extended Disclosure Models A–E, the Disclosure Review Document); CPR Part 31 and PD 31B govern most other civil claims. Know which applies before the first case management discussion.
- **Metadata is evidence.** Printing, forwarding or drag-and-drop copying alters or destroys it. Collection method is a legal decision with evidential consequences, not an IT chore.
- **Proportionality is the organising principle**, of the rules, of the Disclosure Review Document, and of UK GDPR data minimisation. Targeted, staged, well-documented approaches beat "collect everything".
- **Technology-assisted review is mainstream.** Since *Pyrrho Investments Ltd v MWB Property Ltd* [2016] EWHC 256 (Ch), English courts have endorsed predictive coding; PD 57AD expects parties to consider it, and to justify not using it in larger cases.
- **Cooperation is a duty, not a courtesy.** Both PD 57AD and PD 31B require parties to discuss sources, date ranges, custodians, keywords and formats before the CMC, and the court will ask what was discussed.
- **Know when you need a forensic specialist.** Deleted data, device-level artefacts, authenticity disputes, departing-employee exfiltration and chain-of-custody challenges are digital forensics questions, not review-platform questions.

THE ONE-SENTENCE VERSION

eDisclosure is a defensible, documented, proportionate pipeline for turning your client's sprawling electronic estate into a reviewable, producible, evidentially intact disclosure set, and every stage of that pipeline can be attacked if it is done casually.

§ 0 2 · FIRST PRINCIPLES

What exactly is electronic disclosure? The problem in plain English

Disclosure is the stage of litigation at which each party states which documents exist that are relevant to the issues, and makes them available to the other side, including the documents that harm its own case. It is one of the defining features of English litigation, and it exists so that cases are decided on the evidence rather than on what each party chose to show.

Fifty years ago "documents" meant paper: letters, contracts, board minutes, ledgers. Today a "document" in the procedural rules means **anything in which information of any description is recorded**, and the overwhelming majority of that information is electronic. A modest commercial dispute now routinely involves mailboxes running to hundreds of thousands of messages, Teams and Slack channels, WhatsApp threads spanning work and personal phones, shared drives, SharePoint and Google Workspace, CRM and accounting systems, and cloud backups nobody in the business remembers configuring.

Electronic disclosure, eDisclosure, is the discipline of handling that material lawfully and defensibly. In practical terms it is a **pipeline**:

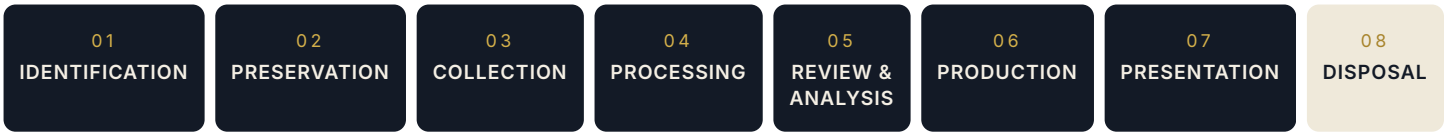

Figure 1 · The eDisclosure lifecycle, adapted from the Electronic Discovery Reference Model (EDRM). Each stage feeds the next; a defect introduced early, a missed custodian, a metadata-destroying copy, propagates through everything downstream.

Four properties of electronic information drive the whole discipline, and none of them has a paper equivalent:

- **Volume.** A single custodian's mailbox can exceed the entire documentary record of a 1990s High Court trial. Human-only review of raw volumes is neither affordable nor accurate; culling, deduplication and technology-assisted review exist to solve this.
- **Volatility.** Electronic data changes and disappears by itself: retention policies auto-delete mail, chat platforms purge messages, phones overwrite storage, employees leave and their accounts are decommissioned. Preservation is therefore urgent in a way paper never was.
- **Duplication and fragmentation.** The same document exists as an attachment in five mailboxes, three drafts on a shared drive and a copy in someone's Downloads folder, while a single WhatsApp conversation is fragmented across two handsets and a cloud backup.
- **Hidden content and metadata.** Every file carries information about itself, authors, dates, revision history, sender routing, GPS coordinates, that the user never sees but which can decide authenticity, chronology and attribution disputes.

§ 0 3 · THE CORE DISTINCTION

How eDisclosure differs from simply exchanging documents

The most common question we are asked by lawyers new to the field is some version of: *"We've always exchanged documents, the client emails us the relevant files, we put them in a bundle. Why is this different?"* It is different in kind, not merely in scale, for six reasons.

DIMENSION	"SIMPLY EXCHANGING DOCUMENTS"	EDISCLOSURE DONE PROPERLY
Scope of "document"	The files the client thinks are relevant and chooses to send.	All ESI within the agreed scope wherever it resides, mailboxes, chat, mobile, cloud, legacy systems, including material adverse to the client, drafts, and deleted-but-recoverable data where ordered.
Who selects	The client self-selects; nobody can verify completeness.	A documented, repeatable methodology (custodians, sources, date ranges, search terms, sampling, TAR) that can be explained to the court and tested by the opponent.
Metadata	Destroyed or altered in transit: printing, PDF conversion, drag-and-drop copying and email forwarding all overwrite dates, authors and system information.	Preserved through forensically sound collection; produced natively or with agreed metadata fields so chronology and authorship can be tested.
Integrity	No hash values, no chain of custody; authenticity rests on assertion.	Hash-verified copies, custody logs and processing reports; any alteration is detectable and the exercise is reproducible.
Duplicates & families	The same email produced five times, attachments separated from parent messages, threads broken.	Deduplication, email threading and family relationships maintained, so review is cheaper and the record coherent.
Court expectations	Exposes the party to criticism, adverse costs orders and, in bad cases, allegations of suppression or spoliation.	Meets the express requirements of PD 57AD / PD 31B: early discussion of sources and formats, completed Disclosure Review Document or EDQ, disclosure certificates signed with confidence.

Put shortly: exchanging documents is an **output**. eDisclosure is the **defensible process** that legitimises the output. The court and the opponent are entitled to interrogate the process, which custodians, which sources, which searches, who decided, and why, and "the client sent us what they had" is not an answer that survives scrutiny.

FOR THE PRACTITIONER

The disclosure certificate is signed by the client, but the solicitor owes independent duties: to take reasonable steps to ensure the client understands and complies with its disclosure duties, and to advise on preservation at the outset. In *Woods v Martins Bank* territory and ever since, "my client only gave me these" has never protected the firm. If the process was casual, the certificate is exposed, and so is the signatory.

§ 0 4 · THE MAP OF THE TERRITORY

eDisclosure and its neighbours

Four adjacent disciplines are routinely confused with eDisclosure. They overlap, share tools and often share providers, but they answer different questions, and instructing the wrong discipline wastes money or destroys evidence.

eDisclosure vs ordinary document disclosure

Ordinary disclosure is the *legal obligation*: the duty, under whichever regime applies, to disclose documents falling within the ordered scope. eDisclosure is the *operational discipline* for performing that obligation on electronic material. The obligation is identical whether a document is a paper letter or a Teams message; what changes is everything about how you find, preserve and produce it.

eDisclosure vs digital forensics

eDisclosure works with **live, accessible data** at scale: it asks "of these two million documents, which must be disclosed?" Digital forensics works at **device and artefact level**, often on much smaller datasets, and asks "what actually happened on this machine?", recovering deleted material, examining registry entries, USB connection records, log files and metadata anomalies, and giving expert evidence about authenticity, attribution and chronology under CPR Part 35 or CrimPR Part 19. A review platform cannot tell you whether a contract was backdated; a forensic examiner can. Conversely, a forensic laboratory image of every custodian's laptop is rarely a proportionate way to run mainstream disclosure. The disciplines meet where disclosure raises forensic questions: suspected deletion, authenticity challenges, exfiltration by departing employees, or a need to collect from locked or damaged devices.

eDisclosure vs document review

Review is one stage *inside* the eDisclosure lifecycle: the assessment of processed documents for relevance, issue-coding and privilege, whether by human reviewers, technology-assisted review, or both. A well-run review cannot rescue a badly scoped identification or a metadata-destroying collection. Treating "eDisclosure" as synonymous with "hiring reviewers" is how parties come to review vast, badly culled datasets at first-class prices.

eDisclosure vs information governance

Information governance is what the client does *before any dispute exists*: retention schedules, data maps, archiving policy, leaver processes, records of which systems hold what. Good governance makes disclosure faster, cheaper and safer; poor governance is why nobody can say where the 2019 project files live. It is also where UK GDPR storage-limitation duties are discharged. The lawyer's interest is practical: a client with a current data map can complete the Disclosure Review Document in days rather than months.

DISCIPLINE	CORE QUESTION	TYPICAL OUTPUT	GOVERNING FRAMEWORK
Document disclosure	What must legally be disclosed?	Disclosure list / certificate, produced documents	PD 57AD, CPR 31, CPIA 1996

eDisclosure	How do we perform disclosure on ESI defensibly and proportionately?	Preserved, collected, processed, reviewed, produced dataset with audit trail	PD 57AD / DRD, PD 31B, EDRM practice
Digital forensics	What happened on this device / is this document authentic?	Forensic images, artefact analysis, expert report and testimony	CPR 35 / CrimPR 19, NPCC principles, FSR Code, ISO 17025
Document review	Which processed documents are relevant / privileged?	Coded review set, privilege log	Instructions, protocol, professional duties
Information governance	What data do we hold, where, and for how long?	Data maps, retention schedules, disposal records	UK GDPR / DPA 2018, sector rules

§ 0 5 · CONSEQUENCES

Why it matters legally: duties, rules and sanctions

eDisclosure failures are not technical embarrassments; they are breaches of duties owed to the court, with a well-stocked armoury of sanctions behind them.

The duties

- **Preservation.** Under PD 57AD para 4, once proceedings are commenced, or a person knows it is or may become a party to proceedings that have been or may be commenced, it must take reasonable steps to preserve documents in its control that may be relevant. That expressly includes suspending document-deletion or destruction processes, sending written notifications to relevant employees and former employees, and taking reasonable steps so that agents or third parties who may hold documents do not destroy them. Solicitors must obtain written confirmation that the client has done this. The common-law position outside the B&PCs is to similar effect: destruction of documents once litigation is contemplated risks adverse inferences, strike-out where a fair trial is imperilled, and contempt.
- **Candour about adverse material.** PD 57AD imposes a freestanding duty, independent of any order, to disclose **known adverse documents**. Under CPR 31 standard disclosure, documents which adversely affect the disclosing party's own case must be disclosed. Criminal disclosure under CPIA 1996 is built entirely on the prosecutor's duty to disclose material capable of undermining the prosecution case or assisting the defence.
- **Reasonable search and honest certification.** Disclosure statements and certificates are signed statements to the court about the search performed. Signing one that describes a search which was not in fact performed engages contempt territory.
- **Cooperation.** PD 31B requires parties to discuss the use of technology and disclosure of electronic documents before the first CMC, using the Electronic Documents Questionnaire where appropriate. PD 57AD embeds cooperation in the jointly completed Disclosure Review Document. Refusal to engage is itself sanctionable conduct.

The sanctions

FAILURE	REALISTIC CONSEQUENCES
Late or incomplete disclosure	Adverse costs orders (including on the indemnity basis), relief-from-sanctions applications, adjourned trials, orders for redone searches at the defaulting party's cost.
Destruction / spoliation	Adverse inferences at trial; strike-out of statements of case where a fair trial is no longer possible; contempt proceedings in serious cases.
False disclosure statement or certificate	Contempt of court proceedings against the signatory; professional conduct referral for the lawyers involved.
Metadata-destroying or unverifiable handling	Authenticity challenges, exclusion or diminished weight of exhibits, cost of forensic remediation, cross-examination of the process itself.
Criminal disclosure failure (prosecution)	Stayed prosecutions, quashed convictions, and the reputational aftermath familiar from the Post Office Horizon litigation and successive disclosure reviews.

Data protection failures in the exercise	ICO enforcement exposure, data-subject complaints, collateral satellite disputes about over-collection of personal data.

FOR THE PRACTITIONER

The recurring judicial theme is that parties are punished less for imperfect results than for **indefensible process**: no hold notice, no record of what was searched, no explanation of who decided what. A contemporaneous methodology memo, sources considered, decisions made, reasons, is the cheapest insurance in the whole exercise.

§ 0 6 · THE RULES

The legal framework: England & Wales, and where the rules differ

Civil claims in the Business and Property Courts: PD 57AD

Practice Direction 57AD (in force 1 October 2022, replacing the Disclosure Pilot in PD 51U) governs most claims in the Business and Property Courts. Its architecture:

- **Initial Disclosure** with statements of case: key documents relied on and those necessary for other parties to understand the claim or defence (subject to limits and agreed dispensation).
- **Extended Disclosure** only where ordered, by reference to **Issues for Disclosure** and one or more of **Models A–E**: A (known adverse documents only), B (limited), C (defined categories requested), D (narrow search-based disclosure, with or without narrative documents), E (wide, *Peruvian Guano*-style, exceptional).
- The **Disclosure Review Document (DRD)**: the jointly completed document recording the Issues for Disclosure, proposed models, data sources, custodians, date ranges, search methodology and the use of analytics or technology-assisted review. Section 2 is, in substance, the parties' eDisclosure plan, and the court manages disclosure through it.
- A simplified regime for **Less Complex Claims** (generally under £1 million or otherwise suitable), with a shortened DRD.
- Express, enumerated **duties** on parties and their legal representatives: preservation, honesty, cooperation, proportionality, and disclosure of known adverse documents.

CURRENT STATUS · 2026

PD 57AD is under active review. The Disclosure Review Working Group chaired by Mr Justice Butcher surveyed the profession between November 2025 and early 2026; the survey summary published in July 2026 records persistent concerns about complexity, front-loaded cost and DRD-driven satellite disputes, alongside recognised benefits in tailoring and earlier engagement. Proposals for simplification are expected to be consulted on in late 2026 or early 2027. Practitioners should check the current text and any transitional arrangements before each CMC, and should expect judicial sympathy for genuinely proportionate, simplified proposals in the meantime.

Civil claims outside the B&PCs: CPR Part 31 and PD 31B

In the County Court and in High Court claims outside the B&PCs, CPR Part 31 continues to apply: standard disclosure (CPR 31.6) or menu-option orders under CPR 31.5(7), the reasonable-search factors in CPR 31.7, and the continuing duty in CPR 31.11. **PD 31B**, Disclosure of Electronic Documents, is the operative text for ESI: it defines electronic documents to include metadata and deleted data, requires discussion of sources, search methods and exchange formats before the first CMC, and provides the **Electronic Documents Questionnaire (EDQ)** as the vehicle for that exchange in larger cases. PD 31B repays reading in full; it is short, and most of the judicial criticism of e-disclosure conduct in Part 31 cases is criticism for ignoring it.

Criminal proceedings

Criminal disclosure rests on the **Criminal Procedure and Investigations Act 1996** and its Code of Practice: investigators must record and retain relevant material; prosecutors must disclose unused material meeting the disclosure test; the defence statement triggers continuing review. The **Attorney General's Guidelines on Disclosure** (revised February 2024, with strengthened guidance on digital materials) address bulk digital exhibits, block-listing strategies, Disclosure Management Documents and defence engagement; CrimPR Part 15 and the Judicial Protocol on unused material complete the picture. Handling of seized devices is governed operationally by NPCC digital evidence guidance, and an independent review of the criminal disclosure regime in the digital age has been examining whether CPIA remains fit for modern data volumes, a live area in which defence practitioners should press for disclosure strategy documents early.

Where the rules differ

FORUM	KEY DIFFERENCES FROM E&W CIVIL DISCLOSURE
Scotland	No general disclosure duty. Documents are recovered by *commission and diligence* on a court-approved *specification of documents*, with the "haver" producing what the specification calls for. Preservation can be secured under s.1 Administration of Justice (Scotland) Act 1972. eDisclosure technique still applies to the recovered material, but the trigger and scope are order-driven.
Northern Ireland	Discovery under the Rules of the Court of Judicature (NI) 1980 remains closer to the pre-CPR *Peruvian Guano* relevance test, typically wider than E&W standard disclosure, with no equivalent of PD 57AD.
Arbitration	Party autonomy governs. Most international tribunals adopt or reference the IBA Rules on the Taking of Evidence (2020): no general disclosure; targeted *requests to produce* (Redfern schedules), with relevance-and-materiality and burden objections. Confidentiality and data-transfer issues loom larger; court-style sanctions are replaced by adverse inferences and costs.
Employment tribunals	Disclosure only as ordered under the ET Procedure Rules, commonly standard-disclosure-style orders by case management order. Volumes are smaller but the same preservation, metadata and format principles apply, and tribunals increasingly see mobile and chat evidence disputes.
Other tribunals / inquiries	Regime-specific: regulatory notices (e.g. FCA, CMA, SFO s.2) and statutory inquiries impose their own production duties, often with prescribed electronic formats and tight deadlines, an eDisclosure exercise in all but name.

§ 0 7 · VOCABULARY

Important terminology

The working vocabulary below is enough to read a Disclosure Review Document, brief a provider and follow a CMC argument. A fuller glossary appears at the end of this guide.

TERM	WHAT IT MEANS IN PRACTICE
ESI	Electronically stored information, every species of electronic document, message, database record and its metadata.
Custodian	A person (or system) whose data holdings are collected, "the CFO's mailbox, laptop and phone" is three sources for one custodian.
Legal hold	The written instruction suspending deletion and requiring preservation of potentially relevant material, issued when litigation is contemplated.
Forensic collection	Capture of data using write-protected, hash-verified methods that preserve metadata and produce a verifiable, reproducible copy.
Hash value	A cryptographic fingerprint (MD5, SHA-256) of a file or image. Identical hashes prove identical data; hashing underpins integrity verification and deduplication.
Processing	Ingesting collected data into a platform: extracting text and metadata, expanding containers (PSTs, zips), de-NISTing system files, deduplicating, indexing, threading emails.
Deduplication	Removing exact duplicates (by hash) globally or per custodian so each document is reviewed once.
Email threading	Grouping a conversation so reviewers read the most inclusive message rather than every intermediate reply.
TAR / predictive coding / CAL	Technology-assisted review: machine-learning ranking of documents by likely relevance, trained on lawyer decisions; continuous active learning (CAL) retrains as review proceeds. Judicially endorsed in England since *Pyrrho* (2016).
Native / near-native / image production	Producing the original file format (native), a converted-but-faithful form, or page images (TIFF/PDF) with extracted text and metadata in a load file.
Load file	The structured index (e.g. DAT/OPT, or platform exchange formats) accompanying a production, mapping documents to metadata fields, text and images.
Redaction	Removal of privileged, irrelevant-confidential or protected personal data from a produced document, performed on the produced form, never by editing the native original.
DRD / EDQ	The Disclosure Review Document (PD 57AD) and Electronic Documents Questionnaire (PD 31B), the two procedural vehicles in which parties record sources, custodians, date ranges, searches and formats.
Models A–E	PD 57AD's menu of Extended Disclosure orders, from known-adverse-documents-only (A) to full train-of-inquiry disclosure (E).

Known adverse documents	Documents a party is actually aware of (without further search) that are contrary to its case on the issues, disclosable under PD 57AD whatever model is ordered.

§ 0 8 · THE LIFECYCLE

The complete lifecycle: identification to disposal

Stage 1 · Identification

Map where potentially relevant ESI lives before deciding what to do with it. Interview the client's IT function and the key custodians themselves, custodians know about the WhatsApp group and the personal Gmail; IT knows about the retention policy and the archived file server. Record systems (email platform, chat, document management, mobile fleet, cloud tenancies, backups, legacy systems), custodians, date ranges and volumes. **What the lawyer should do:** produce a written data map and custodian list; ask expressly about messaging apps, personal devices used for work (BYOD), departed employees, and third parties holding client data (agents, accountants, providers). This map populates DRD Section 2 or the EDQ almost verbatim.

Stage 2 · Preservation

Freeze the identified material against alteration and deletion: written legal-hold notices, suspension of auto-deletion and recycling policies, in-place holds on email and chat platforms, retention of departing employees' devices and accounts, and preservation requests to third parties. Covered in depth in §10. **What the lawyer should do:** issue the hold in writing on day one, diarise reminders, and obtain the written client confirmations PD 57AD expects.

Stage 3 · Collection

Copy the preserved data into the disclosure workflow using methods that maintain metadata and integrity, platform export tools (Microsoft Purview, Google Vault), forensic imaging, or targeted forensic collection from devices and mobiles. Method is dictated by evidential risk: routine mailbox data tolerates administrative export under a documented protocol; a disputed device or a suspected-deletion scenario demands forensic acquisition. Covered in depth in §11. **What the lawyer should do:** decide collection method consciously, per source, and record why; never allow custodians to self-select and forward "the relevant stuff".

Stage 4 · Processing

Collected data is ingested into a review platform: containers expanded, text and metadata extracted, system files de-NISTed, exact duplicates suppressed, emails threaded, and the population indexed for searching. Exceptions (encrypted, corrupt, unsupported files) are logged for decisions, not silently dropped. Culling is applied here: date filters, custodian scope, agreed search terms tested against samples, and analytics such as concept clustering. **What the lawyer should do:** insist on a processing report (volumes in/out at each step, exception log), it is the audit trail behind the disclosure certificate, and test search terms empirically rather than negotiating them as rhetoric.

Stage 5 · Review and analysis

The culled population is assessed for relevance to the Issues for Disclosure, privilege, confidentiality and data-protection redaction needs. Structure the review: a written protocol defining the issues and coding rules; first-level review (human, TAR, or CAL-prioritised); second-level and privilege QC; sampling of the discarded population to validate the methodology. **What the lawyer should do:** keep decision logs; validate TAR with

statistical sampling you can later defend; run privilege screens (law-firm domains, named lawyers) but never rely on screens alone.

Stage 6 · Production

Disclosable documents are exchanged in the agreed format with agreed metadata fields, unique identifiers, redactions burned in, and families intact. Format should have been agreed at the DRD/EDQ stage, spreadsheets and audio-visual material generally in native; correspondence commonly as images plus text plus metadata. **What the lawyer should do:** QC the production before it leaves (sample redactions, check families and privileged withholds), record hash manifests of what was produced, and keep the production set immutable.

Stage 7 · Presentation

Disclosure feeds trial: electronic bundles, chronologies built from metadata, and, where authenticity or provenance is disputed, expert evidence explaining what the artefacts do and do not show. **What the lawyer should do:** preserve the link between the trial copy and the collected original (IDs and hashes), so any challenge can be answered by tracing the exhibit back through the pipeline.

Stage 8 · Disposal

When the matter concludes, the data mountain must come down. Hosting agreements, client retainers and UK GDPR storage limitation all point the same way: agree a retention period, then return or verifiably destroy collections, review sets and productions, keeping only what the file-retention policy and any continuing obligations require. **What the lawyer should do:** deal with disposal in the provider contract at the outset (who deletes what, when, evidenced how), check no preservation duty survives (appeals, related claims, regulatory interest), and obtain destruction certificates.

§ 0 9 · IN PRACTICE

Practical workflow and decision tree

The first fourteen days of a new dispute

WHEN	ACTION
Day 1	Issue the legal hold in writing. Instruct the client to suspend auto-deletion, preserve leavers' accounts and devices, and stop "tidying up". Confirm in writing that this has been done.
Days 1–3	Custodian and IT interviews; draft the data map. Ask specifically about chat platforms, WhatsApp/ Signal, personal devices, cloud tenancies, backups and third-party holders.
Days 3–7	Risk-triage the sources: anything volatile (mobiles, ephemeral messaging, a departing employee's laptop) is collected forensically now, even if broader collection waits.
Days 7–14	Scope the likely disclosure exercise: estimate volumes, identify the applicable regime (PD 57AD vs CPR 31), begin the DRD Section 2 / EDQ, and shortlist providers if external support is needed.
Ongoing	Maintain the methodology memo: every scoping decision, with reasons, dated. Re-issue hold reminders at intervals and on staff changes.

Decision tree: scoping the exercise

QUESTION 1
Is litigation contemplated, threatened or commenced?

YES
Preservation duty is live. Issue the legal hold today; everything else follows. Continue to Q2.

NO, INVESTIGATION ONLY
No disclosure duty yet, but collect to evidential standards anyway: internal investigations have a habit of becoming litigation, and UK GDPR still governs what you gather.

QUESTION 2
Which regime governs?

B&PC CIVIL CLAIM
PD 57AD: Initial Disclosure, Issues for Disclosure, Models A–E, DRD. Diarise DRD milestones against the CMC.

OTHER CIVIL CLAIM
CPR 31 + PD 31B: prepare for the pre-CMC discussion of electronic documents; consider the EDQ.

CRIMINAL / REGULATORY / ARBITRAL
CPIA and AG Guidelines; the notice or tribunal's procedural order. Map deadlines and prescribed formats first.

QUESTION 3
Is any source volatile or forensically sensitive?

YES

Mobiles, chat apps with disappearing messages, leavers' devices, suspected deletion or exfiltration: forensic collection first, before the data changes. Involve a specialist (see §21).

NO

Stable corporate sources: plan a documented, targeted collection via platform tools under protocol.

QUESTION 4

What volume survives sensible culling?

SMALL (< ~20K DOCUMENTS)

Linear human review with a tight protocol may be proportionate.

LARGE

Analytics and TAR/CAL, validated by sampling. Under PD 57AD, be ready to justify *not* using TAR in heavy cases.

QUESTION 5

Does anything in the set raise authenticity, deletion or attribution questions?

YES

That is a digital forensics question: preserve the original medium, stop non-forensic handling, instruct an examiner who can report under CPR 35 / CrimPR 19.

NO

Proceed through review and production, keeping the audit trail intact.

Figure 2 · Five questions that scope ninety per cent of eDisclosure exercises. The order matters: preservation and volatility decisions cannot wait for the CMC.

§ 10 · FREEZING THE RECORD

Preservation: legal holds done properly

Preservation is where more disclosure exercises are lost than anywhere else, because the damage is done before lawyers with disclosure in mind are involved. The duty arises when litigation is contemplated; the data starts disappearing immediately regardless.

WHAT A DEFENSIBLE HOLD LOOKS LIKE

- **Written, specific, acknowledged.** A hold notice identifies the dispute, the categories of material and systems affected, and the conduct required and prohibited, and recipients acknowledge it. A corridor conversation is not a hold.
- **Systems, not just people.** Suspend retention-driven auto-deletion on mail and chat for affected custodians (in-place or litigation holds in Microsoft 365 / Google Workspace); pause device reprovisioning and account deletion for leavers; stop backup-rotation from overwriting relevant snapshots where they are the only copy.
- **Mobile and messaging reality.** WhatsApp, Signal and Telegram live on handsets and personal clouds, not the corporate estate. Disappearing-message settings must be turned off for relevant threads; relevant custodians must be told, in writing, not to delete chats or replace handsets without preservation first. BYOD makes this a negotiation with the individual as data subject, not just an instruction.
- **Former employees and third parties.** PD 57AD expressly contemplates notifying relevant former employees and taking reasonable steps regarding third parties who hold documents for the client, agents, accountants, outsourced IT, providers.
- **Documented and refreshed.** Keep the hold register: who was notified, when, acknowledgments, systems suspended, and periodic reminders. Staleness is the hold's natural enemy.

> **FOR THE PRACTITIONER**
>
> Preservation is not collection. A hold freezes data in place; it does not copy it. Where a source is inherently volatile, a handset that could be lost, a chat with disappearing messages enabled, an ex-employee's cooperation that may evaporate, preservation *means* prompt forensic collection. Deciding which sources need copying now, rather than freezing in place, is the key early judgement call.

§ 11 · DEFENSIBLE CAPTURE

Collection methodology and evidential integrity

Choosing the method

METHOD	APPROPRIATE FOR	WATCH-POINTS
Platform export (Microsoft Purview, Google Vault, Slack export)	Corporate mail, chat and cloud drives in routine civil disclosure.	Run under a written protocol by named operators; export logs retained; understand what each tool includes and omits (versions, some metadata, recoverable items).
Targeted forensic collection	Laptops, file shares and mobiles where scope is known but integrity matters.	Write-blocking or read-only APIs; hash verification at capture; contemporaneous notes of device state.
Full forensic imaging	Devices central to the dispute; suspected deletion, backdating or exfiltration; criminal matters.	Bit-for-bit image with verified hashes preserves deleted and unallocated data for later examination; disproportionate as a default for every custodian.
Custodian self-collection	Almost nothing.	Self-selection is unverifiable, destroys metadata (forwarding, drag-and-drop) and invites the inference that the custodian filtered. Courts have repeatedly criticised it. If unavoidable for a peripheral source, do it under written instructions with the custodian's method recorded.

Chain of custody

Every collected item should be traceable: **what** was collected (source, device identifiers, account), **when** and **by whom**, **how** (tool and version, method, settings), **verification** (hash values at capture, re-verified on transfer), and **where it has been since** (storage, access log, transfers). In a laboratory setting this is a signed, timestamped custody log; in a law-firm setting it is, at minimum, a collection log kept to the same discipline. The point is not ceremony, it is that when opposing counsel asks "how do we know this WhatsApp thread is complete and unaltered?", the answer is a document, not a shrug.

INTEGRITY IN ONE PARAGRAPH

Hash at capture. Verify on every movement. Work only on copies; the collected original is never opened, edited or "cleaned up". Log exceptions instead of fixing them silently. If those four habits are followed, virtually every integrity challenge can be met; if any is skipped, the gap is permanent.

§ 12 · BENEATH THE SURFACE

Metadata: the evidence about the evidence

Metadata is the information a system records about a document: who made it, when, on what, and what has happened to it since. In disputes about chronology, authorship and authenticity, metadata frequently *is* the case.

TYPE	EXAMPLES	LITIGATION USE
File-system metadata	Created / modified / accessed timestamps, path, size	Chronology; backdating challenges; copying and exfiltration analysis
Application metadata	Office author and company fields, revision history, total edit time, track changes; PDF producer and creation chain	True origin of a document; concealed drafts; who really wrote it
Email metadata	Full headers: routing servers, IPs, message IDs, true send times	Authenticity of disputed emails; spoofing; timeline verification
Mobile / chat metadata	Message state, delivery/read markers, deletion traces, attachment records	Completeness of produced threads; manipulation detection
Media metadata	EXIF: device, timestamp, GPS coordinates	Where and when a photograph was really taken

What the lawyer should do: agree the metadata fields to be exchanged in the DRD/EDQ (date sent, author, recipients, filename, hash, family references, and so on); produce spreadsheets and media natively so their metadata and formulae survive; and treat unexplained metadata anomalies in the opponent's production, creation dates after signature dates, single-session "historic" records, missing headers, as cross-examination material and, where serious, grounds for forensic examination.

> **FOR THE PRACTITIONER**
>
> Metadata is also a trap for your own side: a client who "helpfully" opens, re-saves and renames key files before handover has just modified the very timestamps you may need to rely on. The hold notice should say, in terms: *do not open, move, print, forward or re-save potentially relevant files; leave them exactly where they are.*

§ 1 3 · PROTECTED MATERIAL

Privilege and confidentiality

Electronic workflows multiply both the volume of privileged material and the ways to lose it.

- **Screen, then review.** Automated privilege screens, law-firm domains, named in-house and external lawyers, matter references, are essential for triage and never sufficient alone. Legal advice forwarded into commercial threads, lawyers copied on business discussions, and in-house counsel acting in a commercial capacity all defeat mechanical rules.
- **Families and threads.** A privileged attachment on a non-privileged covering email, or one privileged reply buried in a long produced thread, is the classic leak. QC at family level.
- **Redaction discipline.** Redact on the production image, never the native; use tools that remove underlying text (a black rectangle over live text is not a redaction); log every redaction with its basis (privilege, irrelevant-confidential, personal data).
- **Inadvertent disclosure.** Under CPR 31.20, a party who inadvertently allows a privileged document to be inspected needs the court's permission before the receiving party may use it; the receiving lawyer who realises they are reading an obviously privileged document has professional duties too. Agree a clawback protocol in the DRD so the mechanism is contractual as well as procedural.
- **Confidentiality short of privilege.** Trade secrets, third-party confidences and regulatory material may justify redaction, confidentiality rings or controlled-access review, raise it at the CMC, not at production.
- **Provider confidentiality.** Hosting privileged material with a provider does not waive privilege, but the engagement should impose confidentiality, security standards, UK data residency where required, and clear deletion obligations.

§ 1 4 · UK GDPR, data minimisation and the Data (Use and Access) Act 2025

Every eDisclosure exercise is also a personal-data processing exercise: mailboxes and phones are dense with the personal data of custodians, colleagues, customers and bystanders.

- **Lawful basis exists, proportionality is still required.** Processing necessary for legal claims rests on legitimate interests (UK GDPR Art 6(1)(f)), with Article 9(2)(f) and DPA 2018 Schedule 1 conditions available for special category data, and the Schedule 2 paragraph 5 exemption disapplying certain data-subject rights where necessary for legal proceedings, legal advice, or establishing, exercising or defending legal rights. None of this licenses hoovering. Data minimisation (Art 5(1)(c)) maps directly onto disclosure proportionality: targeted custodians, date ranges and sources are both the GDPR answer and the CPR answer.
- **The DUAA 2025.** The Data (Use and Access) Act 2025 (Royal Assent 19 June 2025; principal data-protection provisions commenced 5 February 2026) amends the UK GDPR and DPA 2018: among other things it introduces the "recognised legitimate interests" lawful basis, codifies the reasonable-and-proportionate search standard and stop-the-clock mechanics for subject access requests, and adjusts ICO powers. For disclosure practitioners the immediate relevance is DSAR interaction, parallel subject access requests are a standard litigation tactic, and the codified proportionality standard is now the framework for responding, plus the need to cite the amended legislation accurately.
- **Employee and BYOD data.** Collecting from personal devices engages the custodian's own rights: use targeted extraction (relevant apps, threads and date ranges) rather than full images where possible, give custodians transparency information, and record the balancing exercise.

- **International transfers.** Offshore processing or review requires a transfer mechanism (adequacy, IDTA/Addendum), and watch foreign blocking statutes and local privacy law when collecting from overseas subsidiaries.
- **Security and breach.** A disclosure database is a concentrated, attractive target. Encryption in transit and at rest, access controls, and breach-notification obligations belong in the provider contract.

§ 15 · Proportionality

Proportionality is the test the court will actually apply, in both regimes: the reasonableness factors of CPR 31.7 and PD 31B para 21 (number of documents, nature and complexity, ease and expense of retrieval, significance), and PD 57AD's repeated command that Extended Disclosure be no wider than the Issues for Disclosure require. Practical levers, in rough order of cost-effectiveness:

- **Custodian discipline**, the difference between 8 and 20 custodians is usually the single biggest cost decision in the case;
- **Date ranges** anchored to the pleaded events, not the relationship's full history;
- **Source triage**, inaccessible backups and legacy systems addressed only on demonstrated need, with restoration costs on the table;
- **Tested search terms**, sampled hit counts, iterated, recorded, rather than lists traded like hostages;
- **Staging**, disclose the core first; extend only if the issues survive;
- **Analytics and TAR**, deduplication, threading and prioritised review as the default in volume cases.

Costs are part of the argument: disclosure estimates feed costs budgets, and a party proposing Model D across fifteen custodians should expect to defend the number attached to it.

§ 16 · IN THE WILD

Realistic litigation examples

EXAMPLE 1 · THE SHAREHOLDER DISPUTE AND THE WHATSAPP THREAD

A B&PC unfair-prejudice petition turned on what two directors had agreed informally. The respondent's solicitors listed corporate email only; the DRD stated no mobile data existed. The petitioner's team, whose own client's phone showed years of WhatsApp traffic with the respondents, pressed the point at the CMC. Ordered to address mobile sources, the respondents' late forensic collection revealed one director had deleted the app after the petition was served, but cloud backup artefacts allowed substantial recovery. The deletion, and the DRD's false negative, dominated cross-examination and the costs judgment. **Lesson:** the DRD is a signed statement about sources; "we didn't think of phones" is a preservation failure, not an oversight.

EXAMPLE 2 · THE BACKDATED CONSULTANCY AGREEMENT

In a County Court contract claim, the claimant produced a PDF consultancy agreement dated 2021. Produced only as an image, it looked unremarkable. On a specific-disclosure application the defendant obtained the native file: the PDF's creation chain showed generation in 2024 from a Word document whose revision metadata recorded a single authoring session, three weeks before proceedings issued. The claim settled on receipt of the forensic report. **Lesson:** insist on natives or full metadata for pivotal documents, and treat image-only productions of contested instruments as a red flag.

EXAMPLE 3 · THE LEAVER AND THE CLIENT LIST

An employer suspected a departing salesperson had taken the pricing book. Rather than letting IT "have a look" at the returned laptop, solicitors sent it for forensic imaging. The examination found USB connection records, link files showing the pricing folder opened from the external drive, and cloud-sharing logs to a personal account, evidence that grounded a springboard injunction. In the parallel case where IT had first logged in and browsed the machine, the same artefact types were contaminated with post-return activity and the inference was blunted. **Lesson:** the first hands on a suspect device determine what it can ever prove.

§ 17 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Hold too late, hold too vague.** The notice goes out after the CMC, or says "keep relevant documents" without naming systems, custodians or prohibited conduct.
- **Custodian self-collection.** "Please email us anything relevant", unverifiable, metadata-destroying, and the first thing opposing counsel will attack.
- **Forgetting the phones.** Sources scoped as corporate email plus file shares, in a business that actually runs on WhatsApp.
- **Search terms as negotiation theatre.** Terms agreed without testing; either 4,000 hits (missed material) or 900,000 (unreviewable), discovered after the order is made.
- **Breaking families.** Attachments produced without parents, threads fragmented, hard-copy scans mixed in without unitisation, a record nobody can navigate.
- **Cosmetic redaction.** Black boxes over live text; redacted PDFs with searchable underlay; "redacting" natives.
- **No processing / exception reporting.** Encrypted and corrupt files silently dropped; nobody can say what fell out of the funnel or why.
- **Certifying a search that wasn't done.** The disclosure statement describes methodology aspirationally. This is the mistake with personal consequences.
- **Ignoring disposal.** Terabytes of other people's personal data hosted indefinitely after settlement, with no contractual deletion mechanism.

Technical limitations to understand (and explain to clients)

- **Deleted does not mean recoverable.** Recovery depends on storage type, encryption, time elapsed and overwriting. Modern SSDs (TRIM) and encrypted mobile storage make recovery far less likely than folklore suggests, which is exactly why volatile sources are collected early.
- **Exports are not the whole system.** Platform export tools have documented gaps (certain metadata, versions, recoverable items); know what your tool omits before certifying completeness.
- **Keyword search has floors and ceilings.** OCR errors, misspellings, code words, images of text and audio content all evade keywords; recall is never 100% and should not be certified as such.
- **TAR is only as good as its training and validation.** It ranks; it does not warrant. Statistical sampling of the unreviewed population is what makes the methodology defensible.
- **Encryption may be a wall.** Without keys or lawful compulsion, some material is simply inaccessible; document the attempt and the limitation.
- **Timestamps lie in specific ways.** Time zones, clock drift, and copy operations that reset "created" dates all generate false anomalies, and real anomalies. Interpretation is expert territory.

§ 18 · INTERROGATORIES

Questions to ask

Ask your client

- Where does the business actually communicate, email, Teams, Slack, WhatsApp, SMS, personal accounts? Who uses what?
- What systems hold documents relevant to these issues (DMS, shared drives, cloud tenancies, CRM, finance systems, project tools)? Is there a data map or asset register?
- What are the retention and auto-deletion settings on mail and chat, and have they been suspended for the relevant people?
- Which relevant staff have left or are leaving? Where are their accounts and devices now?
- Are personal devices used for work? Whose, and for what?
- Do third parties hold relevant data, accountants, agents, outsourced IT, providers?
- Has anyone deleted, tidied, exported or "organised" anything since the dispute arose?
- What backups exist, on what rotation, and when would relevant snapshots be overwritten?

Ask your opponent (in DRD/EDQ exchanges or correspondence)

- Which sources, custodians and date ranges were included, and which were considered and excluded, and why?
- When was the preservation step taken, and what did it cover? Were mobile and chat sources preserved?
- What collection methods were used per source, and by whom? Was any self-collection involved?
- What search terms, filters and analytics were applied, with hit counts? What sampling validated them?
- What is the exception report, encrypted, corrupt or unprocessed items, and how were exceptions resolved?
- In what format will production be made, with which metadata fields, and how are families and redactions handled?
- For pivotal documents: will natives be produced, and are hash values available?

Ask a forensic / eDisclosure provider

- What methodology and tools will you use for each source type, and what does each tool *not* capture?
- How are integrity and chain of custody documented, hashing, custody logs, access controls? To what standards (NPCC principles, ISO 17025 alignment, ISO 27001 security)?
- Who will do the work, with what qualifications, and who would sign an expert report if one is needed?
- Where will data be hosted (jurisdiction), how secured, and who else can access it?
- What are the unit costs, collection, processing per GB, hosting per GB per month, review support, and what assumptions drive the estimate?
- What are your reporting deliverables: collection logs, processing reports, exception logs, search-term reports, production manifests?
- What happens at the end, return, deletion, certification, and on what timetable?

- Can you give evidence, and have your examiners been cross-examined before?

§ 19 · DRAFTING AIDS

Suggested wording for instructions

LEGAL HOLD NOTICE (CORE OPERATIVE PARAGRAPHS)

"With immediate effect, you must preserve, and must not delete, alter, move, forward, print, re-save or otherwise interfere with, any documents or data that relate or may relate to [the dispute], wherever held. This includes emails and attachments, calendar entries, instant messages and chats (including Teams, Slack, WhatsApp, Signal and SMS, on any device including personal devices used for work), documents and spreadsheets in any location, voicemails, photographs, and data held in cloud or third-party accounts. Automatic deletion, archiving and disappearing-message functions affecting such material must be disabled. Do not attempt to 'organise' or select material: preservation means leaving it exactly where and as it is. Please confirm in writing by [date] that you have read and will comply with this notice."

INSTRUCTION TO AN EDISCLOSURE / FORENSIC PROVIDER

"We instruct you to collect the sources listed in Schedule 1 using forensically sound, hash-verified methods that preserve metadata, and to document collection in logs sufficient to evidence chain of custody. Please process the collected data (including de-NISTing, deduplication [global/per custodian], and email threading), report volumes and exceptions at each stage, and load the data for review. No original media or source data is to be altered. Search terms and filters are to be applied only as agreed in writing, with hit-count reports before application. Data is to be hosted [in the UK] with encryption in transit and at rest and role-based access. On conclusion, all data is to be [returned/destroyed] and destruction certified. Where examination raises matters requiring expert opinion, any report is to comply with [CPR Part 35 and PD 35 / CrimPR Part 19], including the expert's declaration."

PROPOSAL TO THE OPPONENT ON PRODUCTION FORMAT (FOR THE DRD / EDQ)

"Production is to be made electronically with a load file including the following fields per document: unique ID; family references; custodian; source; date sent/created; author/sender; recipients; filename; file type; MD5 or SHA-256 hash. Emails and standard documents are to be produced as searchable PDF or single-page TIFF with extracted text; spreadsheets, databases, audio, video and any document whose formulae, formatting or metadata may be material are to be produced in native format. Redactions are to be burned in with the basis logged. Documents are to be produced in family groups. Inadvertently produced privileged material is to be dealt with under the clawback provisions at [ ]."

§ 20 · QUICK CONTROL

Checklist and red flags

The eDisclosure checklist

- ☐ Legal hold issued in writing on contemplation of litigation; acknowledgments and client confirmation on file; reminders diarised
- ☐ Data map completed: systems, custodians, date ranges, volumes, third-party holders, BYOD
- ☐ Volatile sources (mobiles, chat, leavers) forensically collected early
- ☐ Applicable regime identified (PD 57AD / CPR 31 + PD 31B / CPIA / tribunal or arbitral rules) and milestones diarised
- ☐ Collection method chosen per source, recorded, with hashes and logs
- ☐ Processing report and exception log received and reviewed
- ☐ Search terms tested against samples; hit counts recorded; methodology memo maintained
- ☐ Review protocol in writing; privilege QC at family level; TAR validated by sampling
- ☐ Production format and metadata fields agreed; families intact; redactions burned and logged; production manifest hashed
- ☐ Data protection addressed: minimisation, transparency where required, transfers, provider security, disposal terms
- ☐ Disclosure statement / certificate accurate against what was actually done
- ☐ End-of-matter disposal executed and certified

Red flags

- **"There are no phones / no chat messages."** In 2026, almost never true. Probe before accepting.
- **Image-only production of a contested instrument**, a signature page PDF with no native, no metadata, no hash.
- **Metadata anomalies:** creation dates after signature dates; entire "historic" ledgers authored in one session; emails with missing or inconsistent headers.
- **Suspiciously clean datasets:** no drafts, no internal candour, gaps precisely bracketing the critical fortnight.
- **Sudden device events after proceedings:** handsets lost, laptops reimaged, accounts "routinely" deleted post-issue.
- **An opponent who cannot describe their own methodology**, no source list, no term testing, no exception report.
- **Your own client "tidying up"**, exporting chats selectively, or resisting the hold. Escalate immediately; the certificate is yours to worry about.
- **Provider red flags:** no hashing, no custody documentation, reluctance to commit deliverables or deletion terms to writing.

§ 2 1 · ESCALATION

When to involve a digital forensic expert

Most disclosure is capably run by solicitors with an eDisclosure platform. A digital forensic specialist earns their fee when the questions move from "which documents?" to "what happened?":

- **Authenticity is disputed**, a contract, email, chat thread, image or recording alleged to be forged, altered or backdated.
- **Deletion is suspected**, recovery from devices, backups and cloud artefacts, and expert interpretation of what deletion traces do and do not prove.
- **Exfiltration and leaver cases**, USB, cloud-sharing and access artefacts to support (or refute) injunctions and misuse claims.
- **Locked, damaged or encrypted sources**, lawful acquisition from devices standard tools cannot reach.
- **Attribution is contested**, who was at the keyboard: logins, device artefacts, malware and remote-access alternatives.
- **Mobile and chat evidence is central**, complete, metadata-intact extraction of WhatsApp and similar platforms, rather than screenshots.
- **The other side's forensics need testing**, independent re-examination of images and methodology in criminal and civil cases alike.
- **The court needs an expert**, CPR Part 35 / CrimPR Part 19 reports, with an examiner who can survive cross-examination.

Instruct early. An examiner involved before collection prevents the contamination that an examiner involved after collection can only describe.

§ 2 2 · COMMON QUESTIONS

Frequently asked questions

What is eDisclosure, and how is it different from simply exchanging documents?

eDisclosure is the defensible process for performing disclosure on electronically stored information: identifying and preserving sources, collecting them without damaging metadata, processing and culling the volume, reviewing for relevance and privilege, and producing in agreed formats with an audit trail. Simply exchanging documents is only the last step of that chain, performed without the process that makes it complete, verifiable and safe to certify. The rules (PD 57AD; PD 31B) assume, and in places require, the process, not just the exchange.

Do we need an eDisclosure exercise in a small case?

You always need the *duties* discharged, preservation, honest search, accurate certification. The machinery scales: a two-custodian dispute may need only a hold notice, a documented mailbox export and a small review database. What never scales down is self-collection by the client and unpreserved phones.

Can we just print the WhatsApps / take screenshots?

Screenshots prove that pixels existed on a screen; they carry no metadata, omit context, and are trivially fabricated, courts and tribunals increasingly say so. Extract chat evidence forensically from the handset or backup so completeness and integrity can be demonstrated.

Is technology-assisted review accepted by the courts?

Yes. English courts approved predictive coding in *Pyrrho* (2016) and have treated it as unexceptional since; PD 57AD's DRD asks parties to state whether they will use analytics and TAR, and larger parties may be pressed to justify not using it. The defensibility question has moved from "may we?" to "how was it validated?"

Who pays for all this?

Each party generally bears its own disclosure costs, subject to costs budgeting and the ultimate costs order, but disproportionate demands can be met with applications to shift or cap costs, and disclosure conduct (good and bad) is regularly reflected in costs awards. The cheapest lever remains scope: custodians, dates and sources.

What happens to the data when the case ends?

It should be returned or verifiably destroyed under the provider contract and the client's retention policy, subject to any surviving obligation (appeal windows, related proceedings, regulatory holds). Indefinite hosting of a litigation database full of third-party personal data is a data-protection liability with a monthly invoice attached.

§ 2 3 · REFERENCE

Glossary

BYOD
Bring your own device, personal hardware used for work, complicating both preservation and privacy.

CAL
Continuous active learning, TAR that retrains on every coding decision, feeding reviewers the likeliest-relevant documents first.

Chain of custody
The documented, unbroken record of who has held evidence, when, and what was done to it.

Culling
Reducing the collected population before review: date filters, deduplication, de-NISTing, search terms.

Custodian
A person or system whose data is within scope for preservation and collection.

De-NISTing
Removing known system files (by reference to the NIST hash library) from a processed dataset.

DRD
Disclosure Review Document, the joint PD 57AD document recording issues, models, sources and methodology.

EDQ
Electronic Documents Questionnaire, PD 31B's schedule for exchanging information about e-documents.

EDRM
Electronic Discovery Reference Model, the standard lifecycle map from information governance to presentation.

ESI
Electronically stored information.

EXIF
Embedded metadata in images: device, timestamp, frequently GPS.

Family
A parent document and its attachments/embedded items, kept together through review and production.

Forensic image
A verified bit-for-bit copy of a storage device, including deleted and unallocated space.

Hash (MD5 / SHA-256)
A cryptographic fingerprint used to verify integrity and identify duplicates.

Known adverse documents
Documents a party is aware of that are contrary to its case, disclosable under PD 57AD regardless of model.

Legal hold
The written preservation instruction issued when litigation is contemplated.

Load file
The structured index accompanying a production, mapping documents to metadata, text and images.

Metadata
System- and application-recorded information about a document: dates, authors, routing, history.

Native format
The file in its original application format, metadata and functionality intact.

Processing
Preparing collected data for review: extraction, expansion, deduplication, indexing, threading.

Redaction
Irreversible removal of protected content from a produced document.

Spoliation
Destruction or alteration of evidence a party was obliged to preserve.

TAR
Technology-assisted review, machine-learning classification of documents by likely relevance.

Unallocated space
Disk areas not assigned to live files, where deleted material may persist until overwritten.

Authoritative UK references

- Practice Direction 57AD, Disclosure in the Business and Property Courts, incl. the Disclosure Review Document: justice.gov.uk/courts/procedure-rules/civil/rules/practice-direction-57ad

- CPR Part 31, Disclosure and Inspection of Documents: justice.gov.uk/courts/procedure-rules/civil/rules/part31
- Practice Direction 31B, Disclosure of Electronic Documents (incl. the EDQ): justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b
- CPR Part 35, Experts and Assessors: justice.gov.uk/courts/procedure-rules/civil/rules/part35
- Criminal Procedure and Investigations Act 1996: legislation.gov.uk/ukpga/1996/25
- Attorney General's Guidelines on Disclosure (rev. 2024): gov.uk/guidance/attorney-generals-guidelines-on-disclosure-2024
- CPS Disclosure Manual: cps.gov.uk/legal-guidance/disclosure-manual
- Data Protection Act 2018: legislation.gov.uk/ukpga/2018/12 · Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/21
- ICO, UK GDPR guidance and resources: ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources
- Forensic Science Regulator, Code of Practice: gov.uk/government/publications/forensic-science-regulator-code-of-practice
- Judiciary, Review of Disclosure in the Business and Property Courts (survey summary, July 2026): judiciary.uk
- *Pyrrho Investments Ltd v MWB Property Ltd* [2016] EWHC 256 (Ch): bailii.org/ew/cases/EWHC/Ch/2016/256.html
- IBA Rules on the Taking of Evidence in International Arbitration (2020): ibanet.org/resources

DISCLAIMER

This publication provides general information about electronic disclosure practice in the United Kingdom as at August 2026. It 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. Procedural rules, guidance and legislation referred to here change; always check the current text. Links are provided for convenience and were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Since 2007 our London laboratory has supported solicitors, barristers, in-house teams and litigants across the disclosure lifecycle described in this guide. Through **e-discovery.uk** we provide defensible preservation and forensically sound collection (including mobile, chat and cloud sources), processing with full volume and exception reporting, hosted review with analytics and technology-assisted review, and production in court-compliant formats, with hash verification and chain-of-custody documentation from first contact to final production. Where disclosure raises forensic questions, deleted data, authenticity, attribution, exfiltration, the same laboratory provides examination and CPR Part 35 / CrimPR Part 19 expert reports, and our examiners attend court to defend their methodology when instructed. 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