



• CFL ELECTRONIC EVIDENCE SERIES ——— FLAGSHIP GUIDE • 2026 EDITION

The Complete Guide to eDiscovery and eDisclosure

From the first preservation notice to the final trial bundle: a UK-first handbook for litigation teams, with a working comparison to United States practice.

CUSTODY LOG • THE TEN STAGES COVERED IN THIS GUIDE				• LIVE
01 Govern Retention and readiness	02 Identify Custodians and sources	03 Preserve Legal hold and suspension	04 Collect Forensically sound copies	05 Process Extract, cull and index
06 Assess Early case assessment	07 Review Relevance and privilege	08 Produce Lists, natives, load files	09 Present Bundles and expert evidence	10 Dispose Return, delete, certify

About this guide

An original publication by the digital forensic and eDiscovery team at Computer Forensics Lab, for solicitors, barristers, in-house counsel, paralegals, investigators and litigation support professionals who need to run electronic disclosure properly, not merely describe it.

What this guide does

Most introductions to eDiscovery are written for the United States, where the Federal Rules of Civil Procedure, litigation holds and subpoenas set the vocabulary. Lawyers in England and Wales work under a different rulebook: CPR Part 31, Practice Direction 31B and, in the Business and Property Courts, Practice Direction 57AD. This guide covers the whole lifecycle from that English starting point and then shows, stage by stage, where United States practice diverges, because so many matters now touch both systems.

It is written to be used. Each section explains the problem in plain English, says why it matters legally, and sets out what a lawyer should actually do. Part Five collects the working tools.

Three ways to read it

01 New to electronic disclosure

Read Part One in order. Sections 01 to 04 give you the vocabulary, the English rules, the comparison with the United States and the ten stage lifecycle that organises everything else.

02 In the middle of a matter

Go to the stage you are in (Parts Two and Three follow the lifecycle), then test what has been done against the checklist in Section 27 and the red flags in Section 23.

03 US counsel or a cross-border team

Start with Section 03 (the two systems compared), Section 15 (documents held by non-parties) and Section 16 (how US discovery meets UK data protection and the Hague Evidence Convention).

Conventions used

Four kinds of box recur. **PRACTICE POINT** a habit that experienced disclosure teams adopt. **CASE NOTE** an authority and the proposition it is cited for. **RED FLAG** a warning sign that should change what you do next. **US COMPARISON** how federal practice in the United States treats the same point.

“eDiscovery” is used as the umbrella term for the discipline, because that is what the market and the technology call it. “Disclosure” is used for the procedural step in England and Wales. “PD57AD” means Practice Direction 57AD and “the DRD” the Disclosure Review Document. Figures in examples are illustrative.

STATUS OF THE LAW: TWO 2026 CHANGES TO KNOW

A new rule for documents held by others. CPR 31.12A, in force from 6 April 2026 and mirrored in PD57AD paragraph 18.5, lets the court order a party to *request* documents from a person who is not a party. It is covered in Section 15.

A new name for the court. From 1 October 2026 the Chancery Division becomes the Business and Property Division of the High Court, and the Commercial Court, the Admiralty Court, the Circuit Commercial Courts and the Technology and Construction Court move into it. PD57AD is retitled “Disclosure in the Business and Property Division”; its substance is unchanged, and this guide keeps the familiar phrase “Business and Property Courts”. A working group is separately reviewing PD57AD (Section 02).

Table of contents

About this guide	02
Who it is for, three reading routes, conventions and the two 2026 rule changes to know	
Executive summary	05
The seven things that matter most	
PART ONE • FOUNDATIONS	
01 What eDiscovery is, and what England calls it	07
Vocabulary, anatomy of an email as evidence, why electronic material is different, legal duties, who does what	
02 The English rulebook: Part 31, PD31B and PD57AD	10
Which regime applies, Part 31 essentials, PD57AD architecture and Models A to E, reform watch, sanctions	
03 Two systems compared: England and Wales v the United States	13
Two procedural tracks, topic by topic comparison, the US rules to recognise, 2026 US developments, translation table	
04 The lifecycle at a glance	16
Ten stages with rule hooks, EDRM 2.0, three running principles, the funnel in numbers, who does what at each stage	
PART TWO • BEFORE THE DISPUTE AND AT ITS START	
05 Information governance and litigation readiness	19
Defensible deletion, the data map, leavers, personal devices, collaboration platforms, AI assistants, readiness ladder, client checklist	
06 Preservation and legal holds	21
When the duty arises, PD57AD paragraph 4 step by step, the hold cycle, volatility ladder, suspending deletion, hold notices, preservation letters	
07 Where the evidence lives: sources, custodians and alternative paths	24
Evidence source map, eight source families, custodian tiers, control, source architecture and the alternative evidence paths table	
08 Collection: method, metadata and chain of custody	27
Four principles, choosing a method, what careless handling destroys, hashing, custody records, mobile devices, privacy safeguards	
PART THREE • FROM DATA TO DISCLOSURE	
09 Processing and early case assessment	32
The processing pipeline, settings that are legal decisions, assessment dashboard, what to measure and why	
10 Search: keywords, analytics and defensibility	34
Why keywords disappoint, a seven step method, hit reports, Digicel and Voltaire, analytics, technical limits	
11 Document review	36
The review protocol, workflow and escalation, coding panel, quality control, known adverse documents, over-disclosure	
12 Technology assisted review and generative AI	38
Three generations of technology, Pyrrho, Brown and Triumph Controls, how ranked review works, validation statistics, generative AI risks and controls, what to agree	
13 Privilege, confidentiality and redaction	41
English privilege in one page, decision tree, privilege workflow, inadvertent disclosure, confidentiality rings, redaction that works	
14 Production, inspection and presentation	44
Deliverables, production protocol, pre-production checks, testing the other side's disclosure, authenticity, bundles, experts, disposal	
PART FOUR • SPECIAL SITUATIONS	
15 Documents held by non-parties	47
The routes ladder, new CPR 31.12A, CPR 31.17 applications, Norwich Pharmacal, responding as a non-party, the US subpoena compared	
16 Cross-border matters: US discovery meets UK data	50
Westbound and eastbound routes, Hague Convention and the 1975 Act, transfer mechanisms, section 1782, working with US counsel	
17 Data protection in disclosure	52
How the principles apply, the Data (Use and Access) Act 2025, subject access requests as a litigation tool	
18 Costs and proportionality	54
Where the money goes, paragraph 6.4 factor by factor, six cost levers, reading a provider's price, illustrative review costs	

19	Choosing technology and providers	56
	The landscape, a selection scorecard, professional duties when outsourcing	
20	Beyond the High Court: other forums and jurisdictions	57
	Tribunals, family, arbitration, regulators, Scotland, Northern Ireland and criminal proceedings	

PART FIVE • THE TOOLKIT

21	Worked examples	60
	A PD57AD commercial dispute, a team move with data theft, a US request to a UK subsidiary	
22	Common mistakes and technical limitations	62
	Fifteen recurring mistakes; eight things the technology cannot do	
23	Red flags	63
	In your client's account, in the other side's disclosure, in the data itself	
24	When to involve a digital forensic expert	64
	Disclosure question or forensic question, triggers, how to instruct	
25	Questions to ask: client, opponent, provider	65
	Three question banks, 40 questions	
26	Suggested wording	66
	Preservation advice, hold notice, preservation letter, provider instruction, DRD wording for technology assisted review	
27	Master checklist	68
	Stage by stage, from identification to closing the matter	
28	Glossary	69
	Fifty terms in plain English	
29	References and further reading	71
	Rules, legislation, guidance, cases, United States and international sources, with links	
30	How a specialist laboratory can assist	73
	Where forensic and disclosure skills meet; disclaimer	

FIGURES

01	Anatomy of an email as evidence	08	12	The processing pipeline and its exceptions lane	32
02	Finding the disclosure regime for your matter	10	13	Review workflow with quality control and escalation	36
03	One dispute, two procedural tracks	13	14	How continuous active learning finds the relevant documents first	39
04	The ten stages, with the English rule hook for each	16	15	Recall, precision and elusion explained	39
05	The funnel in numbers: an illustrative commercial dispute	17	16	Is this document privileged? A first-pass decision tree	41
06	The litigation readiness ladder	20	17	Routes to documents held by someone who is not a party	47
07	The legal hold cycle	22	18	Evidence across the Atlantic: the routes in each direction	50
08	The volatility ladder: what disappears first	22	19	Where disclosure money goes, and the six levers that move it	54
09	The evidence source map	24	20	Disclosure question or forensic question?	64
10	Choosing a collection method	28			
11	Chain of custody: from source to courtroom	29			

The seven things that **matter most**

If you read nothing else, read this page.

-
- 01** **Preservation comes first, and it is the lawyer's job to start it**
Under PD57AD the duty bites as soon as a person knows it is or may become a party. Under PD31B the solicitor must tell the client to preserve as soon as litigation is contemplated. Suspend automatic deletion before doing anything else.
-
- 02** **The evidence is no longer in the mailbox alone**
Chat, collaboration platforms, mobile devices, cloud systems, audit logs and AI assistant histories now hold the decisive material. Map the sources before scoping the search.
-
- 03** **Collect once, collect properly**
Unsupervised self-collection by the client is the most common cause of failed disclosure. Forensically sound collection preserves metadata, proves integrity and costs less than doing it twice.
-
- 04** **Review is where the money goes, so reduce what reaches it**
Processing, early case assessment, tested search terms and technology assisted review cut volume defensibly. Above 50,000 documents, the DRD expects an explanation if such tools are not used.
-
- 05** **Cooperation and transparency are duties, not courtesies**
Agree sources, date ranges, keywords and review methodology with the opponent early, and record what was agreed. Courts penalise opacity and unilateral choices in costs.
-
- 06** **England is not the United States**
No depositions as of right, narrower issue-based disclosure, costs shifting, an implied restriction on collateral use and an express duty to disclose known adverse documents. Cross-border matters need both rulebooks and a lawful route for the data.
-
- 07** **Know when the question has become forensic**
Deleted data, disputed authenticity, suspected tampering, departing employees and mobile devices call for a digital forensic expert, not a larger review team.
-



PART ONE

Foundations: the vocabulary, the rules and the map

What electronic disclosure is, which rulebook governs your case, how England and Wales differs from the United States, and the ten stage lifecycle that the rest of this guide follows.

01	What eDiscovery is, and what England calls it	07
02	The English rulebook: Part 31, PD31B and PD57AD	10
03	Two systems compared: England and Wales v the United States	13
04	The lifecycle at a glance	16

What eDiscovery is, and what England calls it

Discovery, disclosure, eDisclosure: three names for one obligation. This section fixes the vocabulary and explains why electronic material changed the economics and the risk of litigation.

The problem in plain English

Every dispute is decided on evidence, and almost all modern evidence is electronic. A party to litigation must find the documents that matter, keep them safe, and show them to the other side, including documents that damage its own case. That duty is centuries old. What is new is the material it applies to: a mid-sized company now creates more recorded information in a week than a Victorian business produced in its lifetime, and most of it sits in systems designed to delete it automatically.

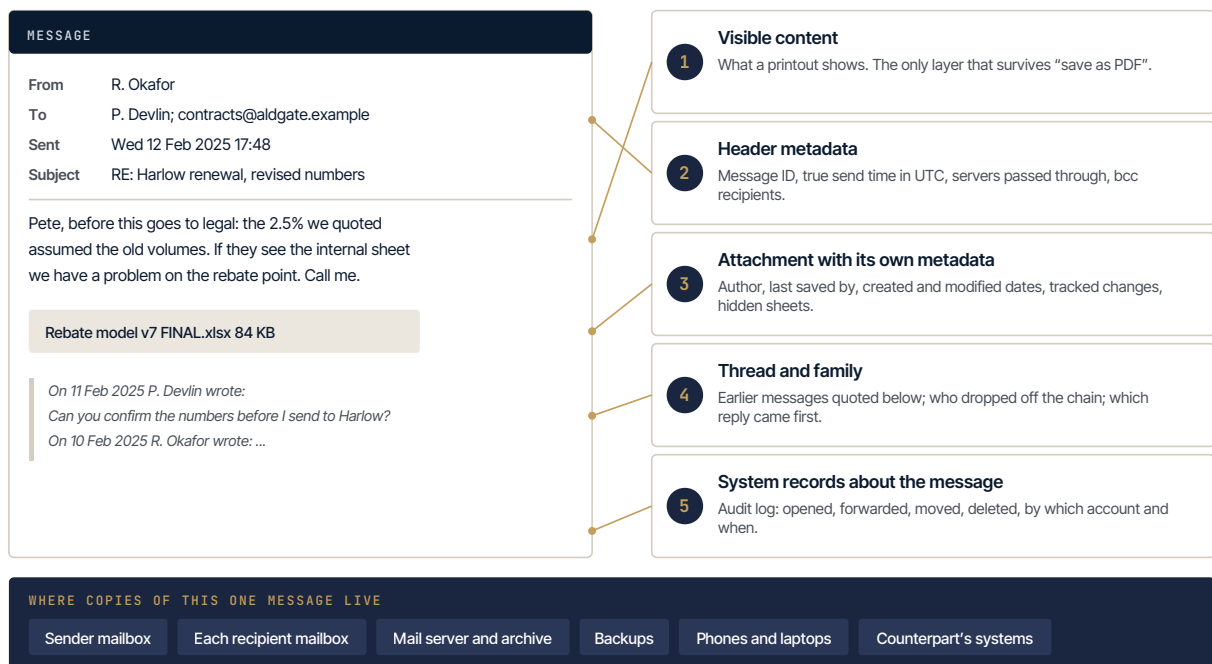
eDiscovery is the discipline of meeting that old duty with modern material. It combines law (what must be preserved, searched for and produced), technology (how data is copied, processed, searched and reviewed) and project management (how to do it on time, within budget and with a record that will survive challenge). When it goes well nobody notices. When it goes badly, trials are adjourned, costs orders are made against the successful party and, occasionally, lawyers are criticised by name.

The vocabulary

TERM	MEANING IN PRACTICE
Disclosure	The English procedural step: stating that a document exists or has existed (CPR 31.2). Inspection is the separate right to see it. Before 1999 English lawyers also said "discovery", and Northern Ireland still does.
Discovery	The United States term, covering document production and also depositions, interrogatories and requests for admission. Far wider than English disclosure.
eDisclosure / eDiscovery	Disclosure or discovery of electronic material, and the industry that supports it. The two words are used interchangeably in the UK market.
Document	"Anything in which information of any description is recorded" (CPR 31.4). PD57AD paragraphs 2.2 to 2.6 spell out that this includes email, text and instant messages, social media, voicemail, audio and video, databases, material on servers and backup systems, deleted data and metadata.
ESI	Electronically stored information: the US term of art (Federal Rule 34), widely used in the UK as shorthand.
Metadata	Data about data: who created a file, when it was modified, who received an email and by what route. Often as probative as the content, and destroyed by careless handling.
Custodian	A person (or shared resource such as a team mailbox) whose data may hold relevant documents.
Control	The test for whose documents a party must search: physical possession, a right to possession, or a right to inspect or take copies (CPR 31.8). It reaches documents held by agents, service providers and, in some circumstances, employees' personal devices.

Why electronic material is different

A paper letter is one object in one place. An email is not. It exists in the sender's mailbox, in every recipient's mailbox, on the mail server, in the archive or journal, in nightly backups and on several phones. Each copy carries metadata that a printout never shows. Five properties follow, and each one drives a part of the process described in this guide.

FIGURE 01 Anatomy of an email as evidence

One message, five layers of evidence and at least six places to find it. Printing it to PDF keeps only the first layer.

PROPERTY	WHAT IT MEANS	WHAT IT DRIVES
Volume	Gigabytes per custodian per year; millions of items in an ordinary commercial dispute.	Processing, culling, analytics and technology assisted review (Sections 09 to 12).
Variety	Email, chat, shared documents, databases, audio, mobile apps, AI assistant prompts and outputs.	Source mapping and collection method (Sections 07 and 08).
Volatility	Retention policies, disappearing messages, device refresh cycles and log rollover destroy data silently.	Immediate preservation and legal holds (Section 06).
Metadata	Hidden data that proves authorship, timing and handling, and that changes if a file is opened or copied carelessly.	Forensic collection and chain of custody (Section 08).
Dispersion	The same document in many places, and different parts of one conversation in different systems.	De-duplication, threading and alternative evidence paths (Sections 07 and 09).

Why it matters legally

Disclosure is a duty owed to the court, policed by the court. A disclosure statement or Disclosure Certificate is signed personally, and a false one made without an honest belief in its truth is a contempt (CPR 31.23; PD57AD paragraph 23). Solicitors carry their own duties: to advise the client on preservation and search, to cooperate with the other side, and under the SRA Code of Conduct not to mislead the court (paragraph 1.4), not to misuse or tamper with evidence (paragraph 2.1), to comply with court orders (paragraph 2.5), and to provide a competent service and keep their knowledge and skills up to date (paragraphs 3.2 and 3.3). That last duty now includes understanding the technology.

CASE NOTE

Earles v Barclays Bank plc [2009] EWHC 2500 (Mercantile). The bank won the case and still lost most of its costs, because it had failed to find and disclose electronic records that would have shortened the trial. Those practising in the civil courts are expected to know the rules on electronic disclosure; in the judge's words, "it is gross incompetence not to".

Cabo Concepts Ltd v MGA Entertainment (UK) Ltd [2022] EWHC 2024 (Pat). The client collected its own documents without supervision and the instructed eDisclosure provider was bypassed. About 40% of the documents (some 800,000) were missed at collection, a failure that began to emerge only three weeks before trial. A four week trial was vacated and indemnity costs followed.

Where the same skills are needed outside litigation

- **Regulatory and internal investigations:** FCA, CMA, SFO and HSE requests use the same collection and review workflow, with tighter deadlines.
- **Arbitration:** document production under the IBA Rules is narrower, but the data is the same.
- **Data subject access requests:** a search, review and redaction exercise governed by UK GDPR, often run alongside a dispute.
- **Employment disputes and team moves:** mobile devices, chat and cloud storage dominate.
- **Criminal proceedings:** the prosecution's disclosure duties under the Criminal Procedure and Investigations Act 1996 now turn largely on digital material.
- **Insolvency and asset recovery:** office holders reconstruct events from seized systems and cloud accounts.

Who does what

ROLE	RESPONSIBILITY
Supervising partner	Owns the disclosure strategy, signs off methodology, answers to the court.
Disclosure lawyer or senior associate	Runs the process day to day: scoping, negotiating with the opponent, review protocol, quality control.
Client's legal and IT teams	Identify custodians and systems, implement the hold, give access. They should not decide what is relevant or run collections unsupervised.
eDisclosure provider	Collection, processing, hosting, analytics, production. Should advise on method and document everything it does.
Review team	First level coding under a written protocol, with escalation routes for privilege and "hot" documents.
Digital forensic expert	Engaged when integrity, deletion, authenticity or device level evidence is in issue (Section 24). May give CPR Part 35 evidence.
Counsel	Advises on issues for disclosure, models, applications and how the documents will be deployed at trial.

KEY POINTS

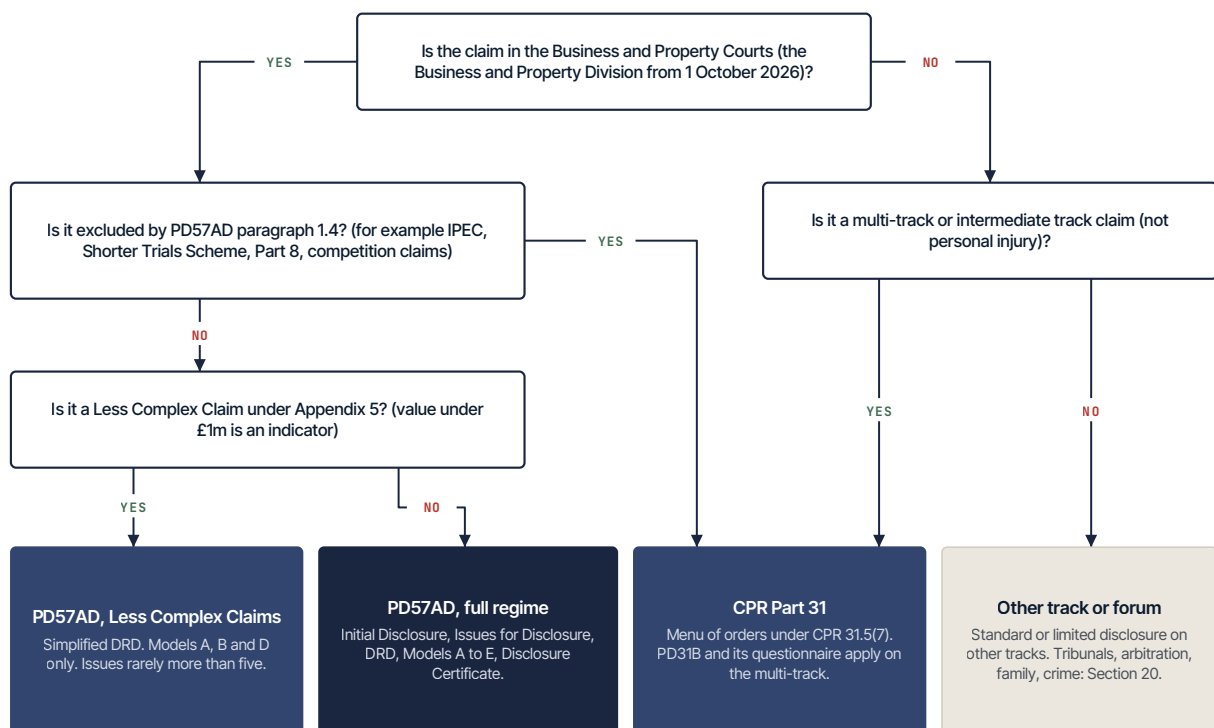
- "Document" means any recorded information, including deleted data and metadata.
- Volume, variety, volatility, metadata and dispersion are the five properties that shape the whole process.
- The duty is owed to the court; lawyers carry personal professional obligations to get it right.

The English rulebook: Part 31, PD31B and PD57AD

England and Wales runs two civil disclosure regimes side by side. The first task in any matter is to identify which one applies, because the duties, documents and deadlines differ.

Which regime applies?

FIGURE 02 Finding the disclosure regime for your matter



Start with the forum. The regime determines when preservation duties arise, what must be exchanged and which forms are used.

CPR Part 31: the general regime

Part 31 governs disclosure in most civil claims outside the Business and Property Courts. Its essentials are:

- **Standard disclosure (CPR 31.6):** documents on which a party relies, documents that adversely affect its own or another party's case, documents that support another party's case, and documents required by a practice direction.
- **The menu (CPR 31.5(7)):** in multi-track and intermediate track claims, other than those including a personal injury claim, the court chooses from a range of orders, from no disclosure, through issue by issue disclosure, to standard disclosure or wider. In those claims standard disclosure is not the default.
- **Reasonable search (CPR 31.7):** the search must be reasonable having regard to the number of documents, the nature and complexity of the proceedings, the ease and expense of retrieval, and the significance of what is likely to be found.
- **Control (CPR 31.8), the disclosure statement (CPR 31.10) and the continuing duty (CPR 31.11),** which lasts until the proceedings end.
- **Specific disclosure (CPR 31.12) and, from 6 April 2026, CPR 31.12A,** under which the court may order a party to request documents from a non-party.

- **Pre-action and non-party disclosure (CPR 31.16 and 31.17)**, covered in Section 15.
- **Inadvertent disclosure of privileged documents (CPR 31.20)** and the **restriction on collateral use (CPR 31.22)**, covered in Sections 13 and 14.

Practice Direction 31B: electronic documents

PD31B applies to claims that are, or are likely to be, allocated to the multi-track. Its most important provisions for day to day practice are:

- **Paragraph 7:** “As soon as litigation is contemplated, the parties’ legal representatives must notify their clients of the need to preserve disclosable documents.” This is a duty on the lawyer, and it arises before proceedings.
- **The Electronic Documents Questionnaire (paragraphs 10 and 11 and the Schedule):** an optional but useful structured exchange covering custodians, date ranges, systems, search methods and preservation, verified by a statement of truth.
- **Reasonable search factors (paragraphs 20 to 24)** and **keyword and automated searches (paragraphs 25 to 27)**, which warn that keyword searching alone may be both over-inclusive and under-inclusive.
- **Metadata (paragraphs 28 and 29)** and **production (paragraphs 32 to 36):** electronic documents should generally be provided in native format in a manner that preserves metadata.

PD57AD: the Business and Property Courts

PD57AD replaced Part 31 for most claims in the Business and Property Courts from 1 October 2022, after a pilot that began in 2019. It was written to break the habit of standard disclosure in every case, and where it applies it displaces most of Part 31: when this guide cites a Part 31 rule and a PD57AD paragraph together, they are alternatives depending on the regime. Its architecture is as follows.

-
- 01 Duties from the moment a dispute is foreseeable (paragraph 3)**
A person who knows it is or may become a party must preserve documents, disclose known adverse documents, search responsibly and conscientiously, act honestly and avoid dumping irrelevant material. Legal representatives must preserve their own documents, advise and assist the client, cooperate with the other side “including through the use of technology”, and satisfy themselves that privilege claims are properly made.
-
- 02 Preservation steps (paragraph 4)**
Suspend deletion, notify employees and former employees in writing, take reasonable steps with agents and third parties, obtain the client’s written confirmation and confirm preservation when serving the particulars of claim or defence. Section 06 sets these out in full.
-
- 03 Initial Disclosure (paragraph 5)**
With its statement of case each party provides the key documents it relies on and those necessary for the other side to understand the case. It can be dispensed with by agreement or where it would exceed the larger of 1,000 pages or 200 documents.
-
- 04 Issues for Disclosure and the DRD (paragraphs 7 and 10)**
The parties identify the key issues that need documents to resolve them, propose a Model for each, and complete the Disclosure Review Document. Section 2 of the DRD is the technical questionnaire: custodians, sources, date ranges, search methods and technology.
-
- 05 Extended Disclosure (paragraphs 6 and 8)**
Ordered issue by issue using Models A to E, only where reasonable and proportionate having regard to the seven factors in paragraph 6.4.
-
- 06 Compliance and production (paragraphs 12 and 13)**
A Disclosure Certificate, an Extended Disclosure List of Documents and production, with electronic documents in native format preserving metadata.
-

07 Policing (paragraphs 11, 17, 18 and 20)

Disclosure Guidance from the court (in practice a short “Disclosure Guidance Hearing”), applications where an order has not been adequately complied with, variation of orders, and sanctions including adverse costs and contempt.

The five Extended Disclosure Models (PD57AD paragraph 8)

MODEL	SCOPE	WHEN IT FITS
A	Known adverse documents only	Issues that turn on law or construction, or where documents will not help. No search is required.
B	Limited disclosure: key documents relied on and those needed to understand the case	Issues where Initial Disclosure essentially suffices. No further search is required.
C	Particular documents or narrow classes, requested by the other party	Targeted gaps: board minutes for a date range, a specific access log. Requests must be precise; vague classes are refused.
D	Narrow search-based disclosure, with or without Narrative Documents	The workhorse for contested factual issues. Each party searches for documents likely to support or adversely affect a case on the issue.
E	Wide search-based disclosure, including train of inquiry documents	Exceptional: fraud, concealment or where a party controls nearly all the evidence.

The Less Complex Claims regime in Appendix 5 offers a simplified route, with a shorter DRD, Models A, B and D only, and an expectation that Issues for Disclosure will rarely exceed five. A claim value under £1,000,000 is an indicator that it may apply, but value is not decisive.

REFORM WATCH

A Disclosure Review Working Group chaired by Mr Justice Butcher surveyed users between November 2025 and February 2026. The summary, published on 29 July 2026, reported 215 responses: only 19% agreed the reforms had succeeded, 67% said disclosure costs had risen, Model D was by far the most used and Models A and E hardly used. A majority (51%) favoured keeping PD57AD with modifications and there was strong support for retaining the known adverse documents duty. The group hopes to consult on recommendations in late 2026 or early 2027. The direction of travel is simplification, not a return to Part 31. Check the current text before relying on paragraph numbers.

What happens when disclosure goes wrong

CONSEQUENCE	SOURCE AND EXAMPLE
Adverse costs, often payable immediately	PD57AD paragraph 20; <i>McParland & Partners Ltd v Whitehead</i> [2020] EWHC 298 (Ch), where the Chancellor warned that parties who fail to cooperate risk immediately payable costs orders.
Loss of costs despite winning	<i>Earles v Barclays Bank</i> (above).
Adjournment or vacated trial	<i>Cabo Concepts</i> (above).
Orders for re-review or independent oversight	<i>Triumph Controls UK Ltd v Primus International Holding Co</i> [2018] EWHC 176 (TCC): an opaque computer assisted review led to an order for manual review of a 25% sample.
Adverse inferences	Drawn where documents have been destroyed or withheld and the court concludes they would have harmed the party responsible.
Strike out and contempt	Reserved for deliberate destruction, forgery or false certificates (CPR 3.4, CPR 31.23, CPR Part 81).
Professional consequences	Wasted costs orders against lawyers (CPR 46.8) and regulatory referral.

KEY POINTS

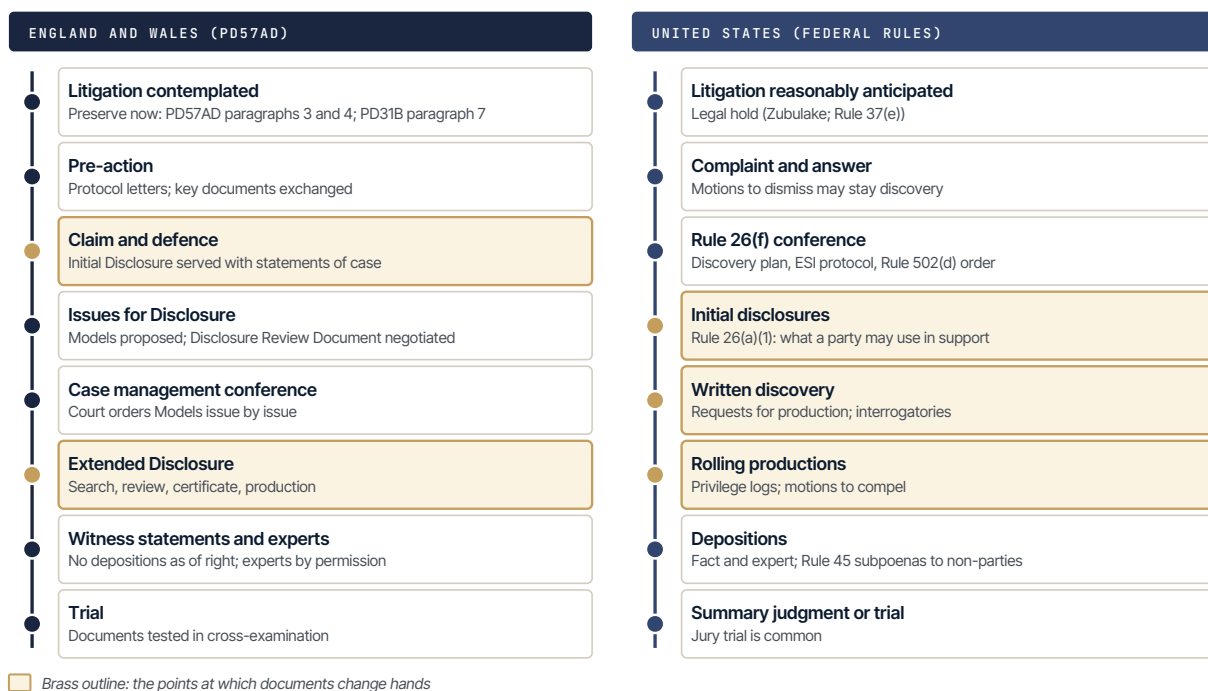
- Identify the regime first: PD57AD in the Business and Property Courts, Part 31 and PD31B elsewhere.
- Both regimes put a personal preservation duty on the lawyer, at or before the start of the dispute.
- Under PD57AD disclosure is ordered issue by issue; Model D is a choice to be justified, not a default.

Two systems compared: England and Wales v the United States

Most eDiscovery technology, vocabulary and case law comes from the United States. English lawyers use the tools daily, so it pays to know exactly where the two systems part company, and where a US habit will mislead an English court.

The shape of a case in each system

FIGURE 03 One dispute, two procedural tracks



In both systems the preservation duty arrives long before any document is exchanged. After that the tracks diverge: England front-loads issues and narrows the search; the United States opens with broad requests and tests the evidence by deposition.

The comparison in detail

TOPIC	ENGLAND AND WALES	UNITED STATES (FEDERAL COURTS)
Scope	Issue-based. Under PD57AD, Extended Disclosure is ordered Model by Model on defined Issues for Disclosure; under Part 31 the court picks from a menu. Train of inquiry disclosure (Model E) is exceptional.	"Any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case" (Rule 26(b)(1)), tested against six proportionality factors.
Preservation trigger	PD57AD paragraph 3.1: a person who "knows that it is or may become a party". PD31B paragraph 7: lawyers must notify clients "as soon as litigation is contemplated".	Common law duty once litigation is reasonably anticipated (the <i>Zubulake</i> line of cases). Loss of ESI is governed by Rule 37(e).
Adverse documents	Express duty to disclose known adverse documents regardless of any order (PD57AD paragraph 3.1(2)); standard disclosure under CPR 31.6 also captures documents adverse to the disclosing party.	No freestanding duty. Initial disclosures cover only what a party may use in support; adverse material emerges through the other side's requests, certification under Rule 26(g) and the duty to supplement.

TOPIC	ENGLAND AND WALES	UNITED STATES (FEDERAL COURTS)
Planning	Disclosure Review Document, discussed between the parties and approved at the case management conference. Electronic Documents Questionnaire under PD31B.	Rule 26(f) meet and confer, producing a discovery plan that must address preservation and form of production; scheduling order under Rule 16(b).
Oral discovery	No depositions as of right. Evidence is given by witness statement and tested at trial. Depositions are possible only by order (CPR 34.8).	Depositions are routine (up to ten per side, one day of seven hours each, under Rule 30), as are interrogatories and requests for admission.
Form of production	Native format preserving metadata (PD57AD paragraph 13.1; PD31B paragraph 33), with searchable text.	As requested or, failing that, as ordinarily maintained or in a reasonably usable form (Rule 34(b)(2)(E)). Negotiated ESI protocols are standard.
Privilege	Legal advice privilege and litigation privilege, each with a dominant purpose test. "Client" is construed narrowly for legal advice privilege. Privileged documents may be listed by class (PD57AD paragraph 14.1).	Attorney-client privilege and work product doctrine. Privilege logs are expected (Rule 26(b)(5)(A)); since 1 December 2025 the parties must address the timing and method of logging in the discovery plan.
Inadvertent disclosure	CPR 31.20 and PD57AD paragraph 19: use only with the court's permission; the obvious mistake test (<i>Atlantisrealm</i> [2017] EWCA Civ 1029).	Clawback under Rule 26(b)(5)(B); non-waiver under Federal Rule of Evidence 502(b); court orders under Rule 502(d) bind in other proceedings.
Collateral use	Automatic: disclosed documents may be used only for the proceedings in which they are disclosed (CPR 31.22), subject to exceptions.	No automatic restriction. Parties negotiate protective orders under Rule 26(c).
Non-parties	Court application under CPR 31.17, a request ordered under CPR 31.12A, a witness summons (CPR 34.2) or Norwich Pharmacal relief. The applicant normally pays the respondent's costs (CPR 46.1).	Subpoena under Rule 45, issued by an attorney without prior court approval. Objections within 14 days; the issuing party must avoid undue burden or expense.
Costs	Costs follow the event (CPR 44.2), so disproportionate disclosure is paid for twice by the loser. Disclosure is a budgeted phase in Precedent H.	Each side generally bears its own fees (the American rule), with limited cost shifting for discovery burdens.
Loss of data	Adverse inferences, costs, strike out in serious cases; destruction before proceedings is judged against the perverting the course of justice standard (<i>Douglas v Hello! Ltd</i> [2003] EWHC 55 (Ch)).	Rule 37(e): curative measures on a finding of prejudice; adverse inference, dismissal or default only on a finding of "intent to deprive".
Review technology	Approved since <i>Pyrrho</i> [2016] EWHC 256 (Ch); the DRD expects an explanation if it is not used above 50,000 documents.	Approved since <i>Da Silva Moore</i> (S.D.N.Y. 2012); described as "black letter law" in <i>Rio Tinto v Vale</i> (S.D.N.Y. 2015). A court will not force a responding party to use it (<i>Hyles</i> , S.D.N.Y. 2016).

The US rules an English lawyer should recognise

RULE	WHAT IT DOES
FRCP 26(b)(1)	Scope and proportionality. The six factors: importance of the issues, amount in controversy, relative access to information, the parties' resources, importance of the discovery, and whether burden or expense outweighs likely benefit.
FRCP 26(b)(2)(B)	ESI that is "not reasonably accessible because of undue burden or cost" need not be produced unless the court orders it for good cause. The nearest English analogue is the reasonableness of the search.
FRCP 26(f)	The parties must confer early and produce a discovery plan covering preservation, form of production and privilege. No discovery before the conference.
FRCP 34	Requests for production, objections stated "with specificity", and the form of ESI production.
FRCP 37(e)	The uniform federal standard, since 2015, for sanctions when ESI that should have been preserved is lost because reasonable steps were not taken and it cannot be restored or replaced.
FRCP 45	Subpoenas to non-parties, with the 100 mile limit on place of compliance and protections against undue burden.
FRE 502(d)	A federal court order that disclosure in the litigation does not waive privilege, effective in any other federal or state proceeding. Routinely sought at the outset.

US DEVELOPMENTS TO WATCH IN 2026

- **Privilege log planning.** Amendments to Rules 16(b)(3) and 26(f)(3), effective 1 December 2025, require the parties to address the timing and method of privilege logging early. New Rule 16.1 on multidistrict litigation took effect the same day.
- **Subpoena reform is pending, not in force.** Proposed amendments to Rule 45 on service and remote testimony cannot take effect before 1 December 2027.
- **AI evidence rules have stalled.** Proposed Federal Rule of Evidence 707 on machine-generated evidence and a draft deepfake provision for Rule 901 were held back for further study in mid-2026. Neither is law.
- **Ephemeral messaging is now a sanctions topic.** In *In re Google Play Store Antitrust Litigation*, 664 F. Supp. 3d 981 (N.D. Cal. 2023), the court found an intent to deprive where chats with history off were not preserved. In *Pable v Chicago Transit Authority* (7th Cir. 28 July 2025) dismissal was upheld after Signal messages were deleted.

A translation table for mixed teams

US COUNSEL SAY	ENGLISH LAWYERS SAY	WATCH FOR
Discovery, production	Disclosure, inspection	English disclosure is a statement that documents exist; inspection is the handing over.
Litigation hold	Preservation notice, legal hold	The English duty has prescribed steps (PD57AD paragraph 4) and written confirmations.
Meet and confer, ESI protocol	DRD discussions, disclosure guidance hearing	The DRD is a court form, filed and approved.
Requests for production	Issues for Disclosure and Models; Model C requests	There is no general right to serve requests.
Privilege log	Withheld documents described in the list, often by class	US counsel may expect document by document entries.
Protective order	CPR 31.22, confidentiality ring or club	English protection is automatic but narrower in one respect: it ends when a document is read in open court unless the court orders otherwise.
Bates number	Disclosure ID or document ID	Agree a numbering convention before the first production.
Spoliation	Destruction of documents	England has no separate tort or uniform rule; remedies are procedural and inferential.
Subpoena duces tecum	CPR 31.17 order or witness summons	An English non-party cannot be compelled without a court order.

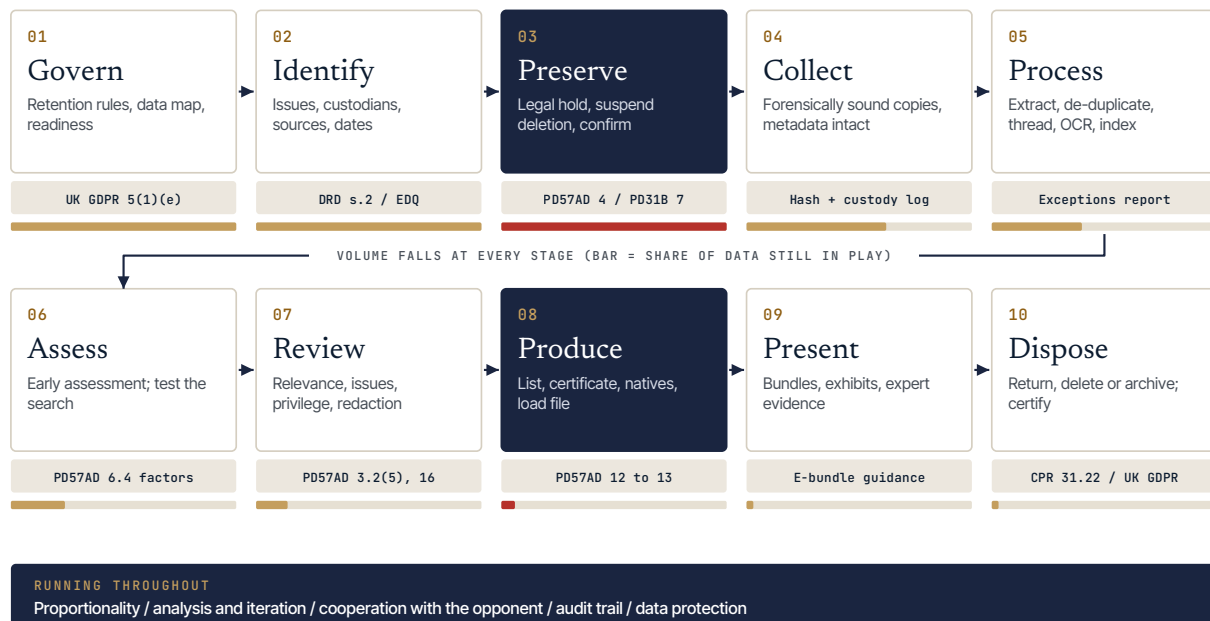
KEY POINTS

- English disclosure is narrower, earlier on issues, and carries an express duty to disclose known adverse documents.
- The United States adds depositions, broad requests and attorney issued subpoenas, and relies on negotiated orders for confidentiality and privilege protection.
- The technology and the forensic disciplines are common to both; the legal wrappers are not. Section 16 deals with matters that cross the Atlantic.

The lifecycle at a glance

Every disclosure exercise, from a two custodian employment claim to a multinational fraud, passes through the same stages. The scale changes; the sequence and the record keeping do not.

FIGURE 04 The ten stages, with the English rule hook for each



Ten stages, one audit trail. Volume should fall at every step; if it does not, the scoping or the search design needs attention.

The industry's shared reference point is the Electronic Discovery Reference Model published by EDRM. A revised model, EDRM 2.0, was released on 1 September 2026: it groups identification, preservation, collection and processing as data acquisition, treats analysis as an activity that runs through every phase, adds disposition as a closing phase and rests the whole on information governance (see edrm.net). The ten stages used in this guide are our own arrangement for English practice and are consistent with it.

Three principles that run through every stage

01 Proportionality

The overriding objective and PD57AD paragraph 6.4 govern every decision: how many custodians, which sources, how far back, which technology. Record the reasoning, because the court will ask for it (Section 18).

02 Iteration

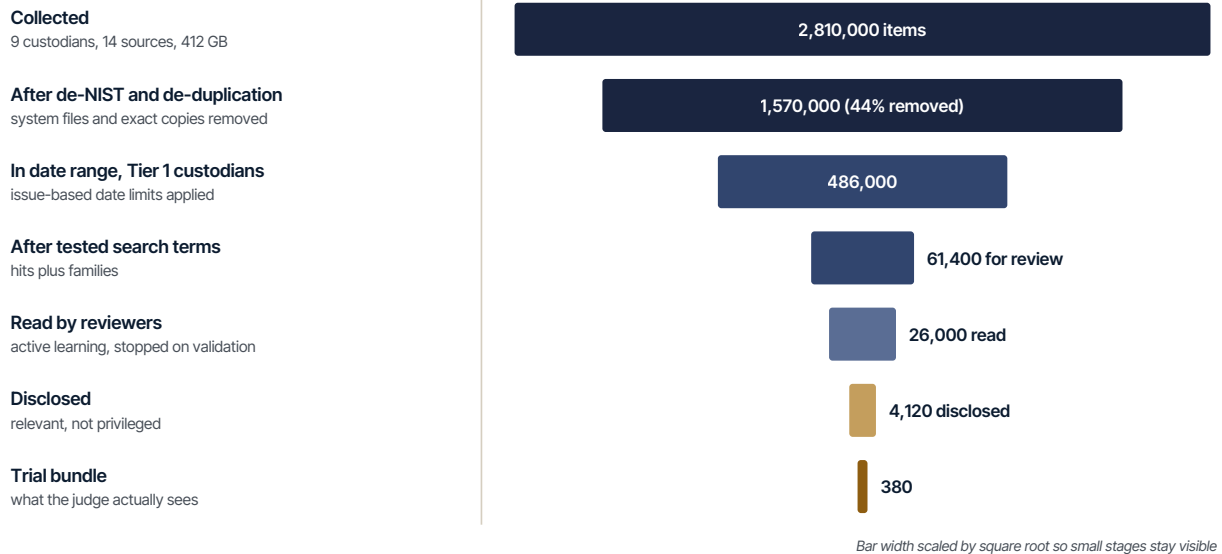
The stages are not a conveyor belt. Review reveals a new custodian; a new custodian means a further collection; early assessment changes the search terms. Build a process that expects to loop.

03 Defensibility

A disclosure exercise is defensible when a competent outsider could read the file and understand what was done, why, by whom and with what result. The audit trail is part of the work product, not an afterthought.

What happens to the volume

FIGURE 05 The funnel in numbers: an illustrative commercial dispute



Illustrative figures for a nine custodian matter. The steepest, cheapest reductions happen before any lawyer reads a document, which is why scoping and processing decisions deserve partner attention.

Stage by stage: who does what, and what record it leaves

STAGE	WHAT THE LAWYER DOES	WHO DOES THE WORK	RECORD CREATED
Govern	Advises on retention, readiness and defensible deletion before any dispute.	Client legal, IT, records	Retention schedule, data map
Identify	Defines issues, custodians, sources and date ranges; interviews key people.	Lawyers with client IT and provider	Custodian register, source map, interview notes
Preserve	Issues the hold, has deletion suspended, obtains written confirmation.	Lawyers, client IT	Hold notices, acknowledgements, suspension log
Collect	Approves method and scope; never delegates to custodians unsupervised.	Provider or forensic examiner	Collection log, hash values, chain of custody
Process	Approves de-duplication, date and file type filters; reads the exceptions report.	Provider	Processing report, exceptions log
Assess	Tests search terms, samples, estimates cost, refines the DRD position.	Lawyers with analysts	Hit reports, sampling results, cost estimate
Review	Writes the protocol, trains reviewers, runs QC, decides privilege.	Review team, supervising lawyers	Protocol, coding history, QC and validation results
Produce	Approves the list, redactions and certificate; checks the production before it leaves.	Provider, lawyers	List of documents, certificate, production log
Present	Builds bundles and exhibits; instructs experts where authenticity or integrity is in issue.	Lawyers, counsel, experts	Bundles, exhibits, expert reports
Dispose	Arranges return, deletion or archive at the end of the matter.	Provider, client	Certificate of destruction, archive record



Before the dispute and at its start

Governance decides how hard disclosure will be. The first fortnight of a dispute decides whether the evidence survives. These four sections cover readiness, preservation, source mapping and collection.

05	Information governance and litigation readiness	19
06	Preservation and legal holds	21
07	Where the evidence lives: sources, custodians and alternative paths	24
08	Collection: method, metadata and chain of custody	27

Information governance and litigation readiness

You cannot preserve what you cannot find, and you should not be keeping what you no longer need. Good governance makes disclosure cheaper, faster and safer, and it is the one stage a client can complete before any dispute exists.

The problem in plain English

Organisations keep too much, in too many places, under nobody's ownership. When a dispute arrives, the first month is spent discovering what systems exist, who administers them and what has already been deleted. Meanwhile data protection law pulls in the opposite direction: personal data must not be kept longer than necessary (UK GDPR Article 5(1)(e)). The answer to both pressures is the same: a written retention schedule that is actually followed, a current map of where information lives, and a rehearsed procedure for suspending deletion when a dispute is foreseeable.

Defensible deletion

There is no general duty in English law to keep documents indefinitely. Routine, good faith deletion under a genuine retention policy, before a dispute is in view, is legitimate and is what the data protection principles require. The position changes once a party knows it is or may become a party to proceedings: from then on PD57AD paragraph 4.1 expressly requires preservation of documents "which might otherwise be deleted or destroyed in accordance with a document retention policy or in the ordinary course of business". Destruction before that point is judged by a stricter test, and sanctions follow only where it amounts to an attempt to pervert the course of justice (*Douglas v Hello! Ltd* [2003] EWHC 55 (Ch)). The lesson for clients: delete on schedule, record it, and have a reliable off switch.

The data map

A data map is an inventory of information systems written for lawyers, not engineers. It need not be elaborate. A spreadsheet that answers the following questions for each system will save weeks.

FIELD	WHAT TO RECORD
System, owner and content	Name, business purpose, internal owner, administrator, external supplier; types of record held, including personal and special category data.
Location	Tenant, region or data centre; on premises or cloud; any copies outside the UK.
Retention	The configured retention period and what happens at expiry (hard delete, soft delete, archive).
Hold capability	Whether deletion can be suspended by user, by date or by keyword, who can do it and how quickly.
Export capability	Native export formats, whether metadata and audit logs are included, and any licence tier needed.
Backups and logs	Backup rotation and age of the oldest restorable copy; audit log retention period.
Leavers	What happens to the account, mailbox, files and device when an employee leaves, and after how long.

Pressure points that cause most damage

Leavers

The custodians who matter most in a dispute have often left. In many Microsoft 365 configurations a departed user's mailbox and OneDrive are deleted around 30 days after the licence is removed unless a hold or retention policy applies, and the laptop and phone are wiped and reissued within days. A leaver procedure should ask one question before anything is deleted: is this person connected to any current or foreseeable dispute, investigation or complaint? If so, preserve the account and image the devices first.

Personal devices and messaging apps

Work is done on WhatsApp, iMessage, Signal and personal email whether or not policy allows it. The Court of Appeal confirmed in *Phones 4U Ltd v EE Ltd* [2021] EWCA Civ 116 that work related material on the personal devices of employees and former employees can fall within a party's control, and upheld an order that custodians be asked to hand their devices to the party's IT consultants, acting under confidentiality undertakings, for searching. A policy that either bans business use of personal channels and enforces the ban, or permits it on terms that include access and retention, is far better than silence.

Collaboration platforms

Teams, Slack and Google Chat are now primary business records. Their retention is set separately from email and is often shorter. Files shared in chats are usually links to a document library, not copies, so the version a recipient saw may differ from the version that exists today unless version history is retained.

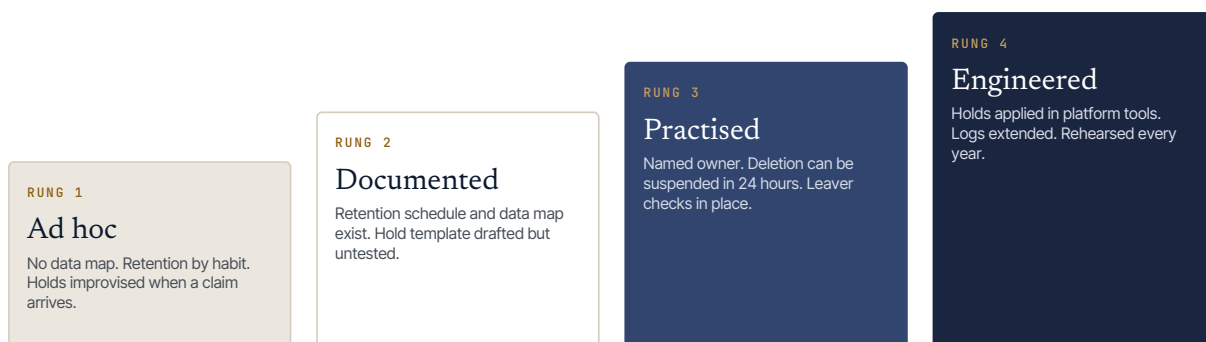
AI assistants, recordings and transcripts

Prompts and responses in tools such as Microsoft 365 Copilot are stored with the user's mailbox data and are searchable with the platform's eDiscovery tools. Meeting recordings, automatic transcripts and AI generated summaries are documents. Decide deliberately whether to create them, how long to keep them, and how their accuracy will be treated, because an unreviewed machine summary of a meeting can be a very awkward disclosable document.

PRACTICE POINT: KNOW THE PLATFORM DEFAULTS

Ask the client's administrator for the actual configured values, not the vendor defaults. As a guide, Microsoft 365 keeps deleted mailbox items in the Recoverable Items folder for 14 days by default (extendable to 30), and audit logs for 180 days (one year for core Exchange, SharePoint and OneDrive records on premium licences). Google Workspace relies on Vault retention rules. Defaults change; record what you find and the date you found it.

FIGURE 06 The litigation readiness ladder



Cost and risk of the first month of a dispute fall with every rung

Most organisations sit on the first or second rung. Moving up one rung typically removes the most expensive month from the next dispute.

A ten point readiness checklist for clients

- ☐ A retention schedule exists, is approved and is applied by the systems, not by memory.
- ☐ A data map exists and was updated in the last twelve months.
- ☐ A named person can suspend deletion everywhere within 24 hours.
- ☐ A template hold notice and distribution list procedure exist.
- ☐ The leaver process includes a disputes check before deletion or device reissue.
- ☐ Policy addresses personal devices, messaging apps and disappearing messages.
- ☐ Audit log retention has been extended to at least one year for key systems.
- ☐ Supplier contracts give rights to data, logs and assistance.
- ☐ Recordings, transcripts and AI assistant histories are covered by the retention schedule.
- ☐ The procedure has been rehearsed once, on a closed matter or a test scenario.

Preservation and legal holds

Preservation is the only stage that cannot be repaired later. A poor search can be rerun and a weak review can be redone, but data that has been deleted is gone. It is also the stage where the rules place the first duty squarely on the lawyer.

When the duty arises

In the Business and Property Courts the duties in PD57AD paragraphs 3.1 and 3.2 apply to a person who “knows that it is or may become a party” to proceedings, whether those proceedings have been commenced or may be commenced in future. That is a low threshold and an early one: it can be crossed by a letter before claim, a threatened termination, a whistleblowing report or a board discussion about suing. Under PD31B paragraph 7 the lawyer’s duty to notify the client arises “as soon as litigation is contemplated”. In both regimes the safe working rule is the same: the moment you are consulted about a dispute that could end in proceedings, preservation advice is the first item of business, and it should be given in writing on day one.

EVENT	DOES IT TRIGGER PRESERVATION?
Letter before claim received or sent	Yes. Proceedings are in view on any reading.
Client instructs solicitors about a dispute	Yes. PD31B paragraph 7 and PD57AD paragraph 4.4 both bite.
Regulator opens an enquiry or requests information	Yes, and separate statutory offences may apply to destruction.
Serious internal complaint, grievance or whistleblowing report	Usually. Treat as a trigger where a claim or investigation is a realistic outcome.
Key employee resigns to join a competitor	Usually. Preserve the devices and accounts before reissue; the cost is trivial compared with the loss.
Ordinary commercial disagreement	Not by itself. Routine retention can continue.

US COMPARISON

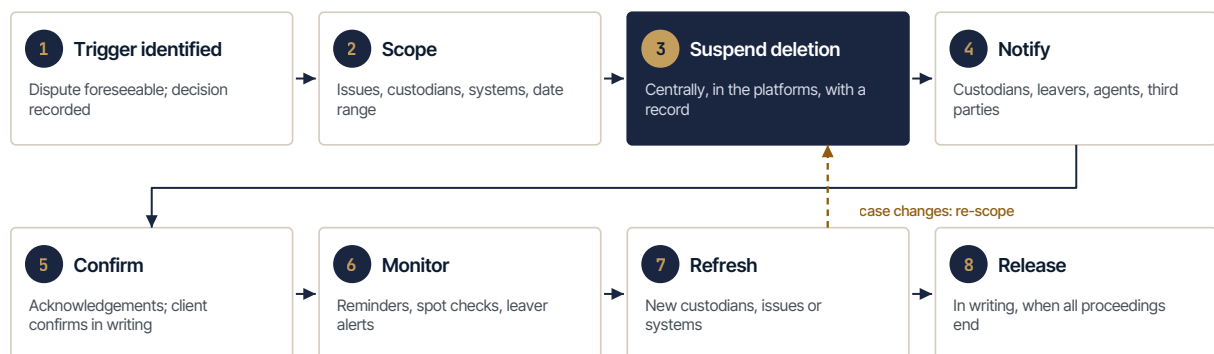
The federal duty arises when litigation is **reasonably anticipated** (*Zubulake v UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003)), and counsel must actively monitor compliance (229 F.R.D. 422 (S.D.N.Y. 2004)). Under Rule 37(e), if ESI is lost because reasonable steps were not taken and it cannot be replaced, the court may order curative measures on a finding of prejudice, but the severe sanctions (adverse inference, dismissal, default) require a finding of intent to deprive. The Sedona Conference Commentary on Legal Holds (2nd edition, 2019) is the standard reference. A UK company with US connections may be subject to both duties at once.

The prescribed steps under PD57AD paragraph 4

PARA	REQUIREMENT	EVIDENCE TO KEEP ON FILE
4.1	Preserve documents that would otherwise be deleted under a retention policy or in the ordinary course of business. Preservation may include making copies.	Note of retention settings before and after suspension.
4.2(1)	Suspend relevant document deletion or destruction processes for the duration of the proceedings.	Administrator’s confirmation, screenshots or change tickets.
4.2(2)	Send a written notification to relevant employees and former employees where there are reasonable grounds to believe they hold disclosable documents not also held by the party.	Distribution list, notice, acknowledgements.
4.2(3)	Take reasonable steps so that agents and third parties who may hold documents on the party’s behalf do not delete or destroy them.	Letters to suppliers, advisers, former advisers.

PARA	REQUIREMENT	EVIDENCE TO KEEP ON FILE
4.3	The notification must identify the documents or classes to be preserved and tell the recipient not to delete them and to take reasonable steps to preserve them.	The notice itself (see Section 26 for wording).
4.4	Legal representatives must, within a reasonable period of being instructed, notify the client of the need to preserve and obtain written confirmation that the steps in 4.2 and 4.3 have been taken.	Your advice letter and the client's written confirmation.
4.5	Each party confirms in writing, when serving its particulars of claim or defence, that preservation steps have been taken.	The confirmation as served.

FIGURE 07 The legal hold cycle



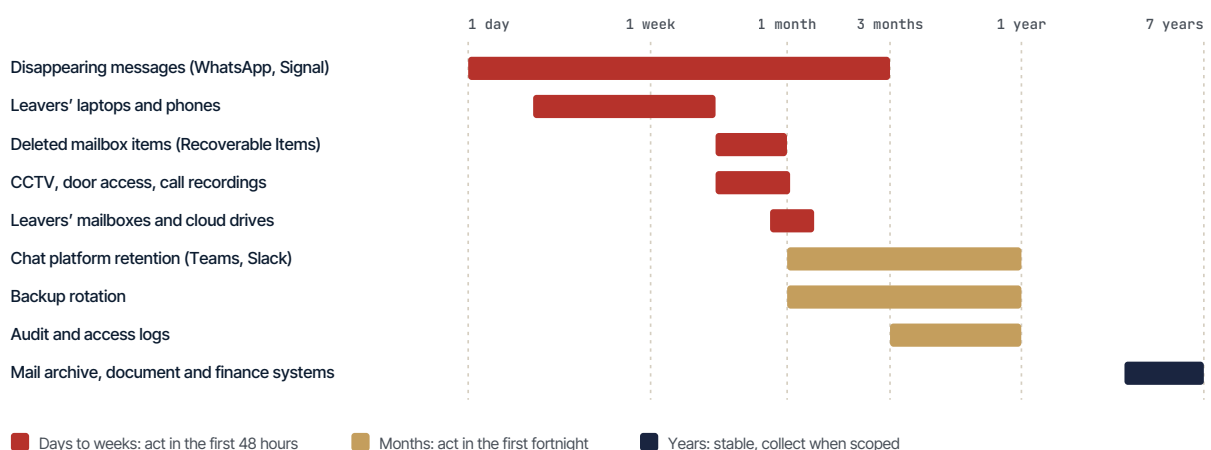
Step 3 before step 4: a hold that depends only on people remembering not to delete is not a hold.

A hold is a process with an owner, not a single email. Most failures occur at steps 5 and 6: nobody checks compliance, and nobody updates the hold when the case changes.

Preserve in order of volatility

Different sources disappear at different speeds. Deal with the fastest first.

FIGURE 08 The volatility ladder: what disappears first



Typical loss windows. Actual periods depend on the client's configuration, which is why the administrator's answers must be obtained in the first week.

What “suspend deletion” means in practice

- ☐ Place custodian mailboxes, OneDrive or Drive accounts and relevant sites on hold in the platform's compliance tools.
- ☐ Suspend or lengthen retention policies for Teams, Slack or Chat channels in scope.
- ☐ Turn off disappearing messages in WhatsApp, Signal and similar apps for relevant chats, and record the date this was done.
- ☐ Stop mobile device management wipes and device reissue for custodians and leavers.
- ☐ Pull and label a backup set before rotation overwrites the period in issue.
- ☐ Extend audit log retention, or export the logs now, and preserve leavers' accounts before licences are removed.
- ☐ Pause clean-up scripts on shared drives; secure call recordings, CCTV and door access data if the facts make them relevant.
- ☐ Ask third parties (managed service providers, accountants, agents, former solicitors) to do the same in writing.

The hold notice

An effective notice is short, specific and written for the person reading it. It should say what the dispute is about in two sentences, which kinds of documents matter, which systems and devices are covered (expressly including personal phones and messaging apps where relevant), what the recipient must stop doing, who to call with questions, and that the obligation continues until released in writing. It should ask for an acknowledgement. Draft it on the assumption that it may be read by the other side. Model wording is in Section 26.

RED FLAG

A hold that relies only on asking individuals not to delete is not a hold. People forget, leave, change phones and, occasionally, have a personal interest in deletion. Wherever a system allows deletion to be suspended centrally, do that first and tell the custodians second.

Monitoring, refreshing and releasing

Diarise reminders (quarterly is common). Reissue the notice when custodians are added, when the issues change after pleadings, and when new systems come to light. Keep a register of who was notified, who acknowledged, and what was suspended. When the matter ends, including any appeal and related claims, release the hold in writing; keeping data under hold indefinitely is itself a data protection problem.

Preservation letters to the opponent and third parties

Where there is a real risk that the other side's data will be lost (a small company, a hostile individual, short retention on a chat platform), write early and specifically: identify the custodians, systems and date ranges you expect to be preserved and ask for confirmation. A specific letter makes it far harder for the recipient to say later that loss was innocent, and it lays the ground for adverse inferences or an application under CPR Part 25 for an interim order preserving the evidence if the risk is acute.

CASE NOTE

Vardy v Rooney [2022] EWHC 2017 (QB). WhatsApp messages and other media were lost through a series of events that the judge found were not accidental, and a phone went into the North Sea. The court drew adverse inferences. The case is a vivid reminder that English courts respond to lost data through inference and credibility findings, without any need for a separate spoliation rule.

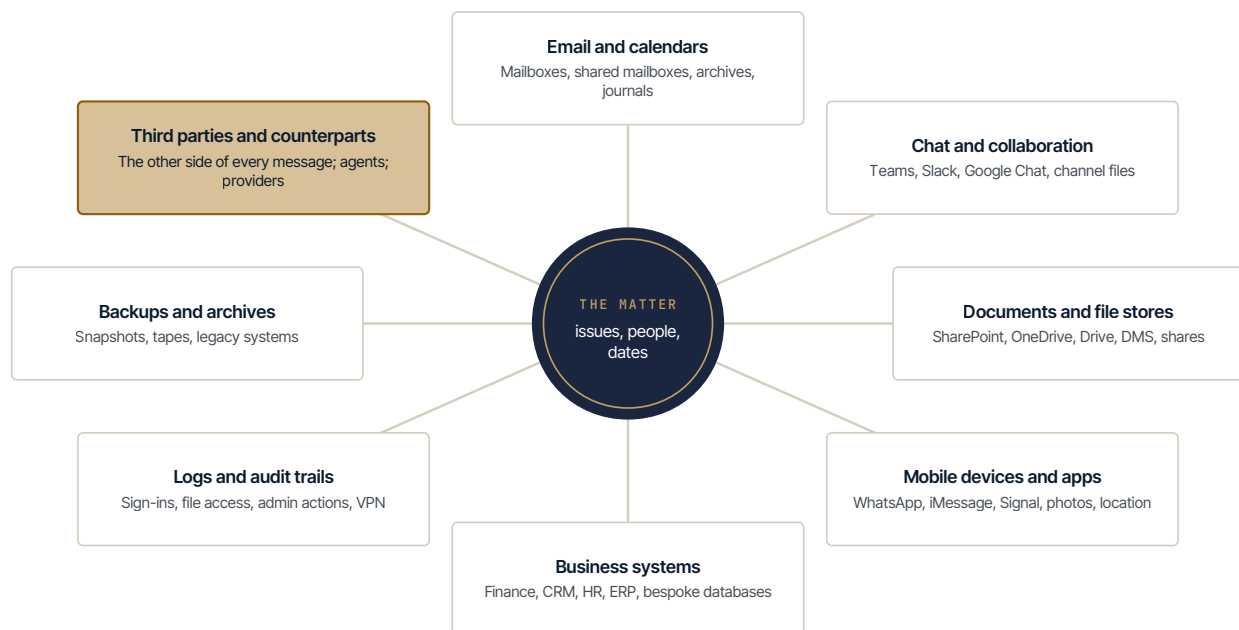
Data protection. Preservation is processing of personal data. The lawful basis will usually be compliance with a legal obligation or legitimate interests (UK GDPR Article 6(1)(c) or (f)). Record the basis and limit access: preservation should be as wide as the risk requires, while access and review should be as narrow as the issues allow (Section 17).

Where the evidence lives: sources, custodians and alternative paths

Identification is the stage at which cases are quietly won or lost. A custodian left off the list or a chat platform nobody mentioned will not be found by any amount of clever review technology later.

Think in source families, not applications

FIGURE 09 The evidence source map



Eight families of source surround every matter. The brass family, third parties and counterparts, is the one most often forgotten and the one that rescues a case when a primary source is lost.

FAMILY	TYPICAL CONTENT	MAIN RISK	USUAL COLLECTION ROUTE
Email and calendars	Messages, attachments, meeting invitations, delegated and shared mailboxes	Leavers' mailboxes deleted; archives and journals overlooked	Platform compliance export with hold
Chat and collaboration	Teams, Slack, Google Chat, channel posts, reactions, edits and deletions	Short retention; linked files that have since changed	Compliance export or vendor discovery API, with linked files and versions
Documents and file stores	SharePoint, OneDrive, Google Drive, network shares, document management systems	Version history trimmed; permissions reveal who could see what	Targeted forensic copy preserving metadata and versions
Mobile devices and messaging apps	WhatsApp, iMessage, Signal, Telegram, SMS, voice notes, photos, location	Disappearing messages, device replacement, encryption, personal ownership	Forensic extraction by an examiner, with consent or order
Business systems	Finance, CRM, HR, ERP, trading and ticketing systems, bespoke databases	No native "document"; reports must be designed and validated	Agreed structured export or report, with a description of the query

FAMILY	TYPICAL CONTENT	MAIN RISK	USUAL COLLECTION ROUTE
Logs and audit trails	Sign-ins, file access, downloads, sharing, admin actions, door access, VPN	Rollover within 90 to 365 days	Immediate export by administrator
Backups and archives	Point in time copies of all of the above	Rotation; cost and time to restore	Isolate the relevant set; restore only if needed and proportionate
Third parties and counterparts	The other side of every conversation; agents, advisers, cloud and managed service providers	Outside your control unless contract or the court gives access	Request, contractual right, CPR 31.12A, CPR 31.17 (Section 15)

Custodians: a tiered register

List everyone who could hold relevant documents, then tier them. The tiers keep preservation wide and review narrow, which is exactly what proportionality requires.

TIER 1 Collect and review Decision makers and direct participants in the disputed events. Usually four to ten people.	TIER 2 Collect and hold People likely to hold unique material on some issues. Collected now, reviewed only if Tier 1 shows gaps.	TIER 3 Preserve only Peripheral contacts. On hold, not collected, revisited if the case changes.
---	--	--

Interview Tier 1 custodians early. Twenty minutes with each will tell you more about where documents are than any system diagram. Ask what tools they really used, which personal devices and accounts touched work, who else was copied, what nicknames and project names were used, and what they have deleted or lost since the events. Record the answers; they feed Section 2 of the DRD directly.

Control: whose documents must you search?

A party must search documents within its control: those it physically holds, those it has a right to possess, and those it has a right to inspect or copy (CPR 31.8; PD57AD Appendix 1). Three situations cause most argument.

- **Personal devices and accounts.** Work material on an employee's own phone is capable of being within the employer's control (*Phones 4U*). Plan for a consent-based, privacy-protective collection through an independent examiner.
- **Group companies.** A parent does not automatically control a subsidiary's documents, or the reverse (*Lonrho Ltd v Shell Petroleum Co Ltd* [1980] 1 WLR 627). Control can nonetheless arise from an arrangement or understanding that documents will be provided on request (*North Shore Ventures Ltd v Anstead Holdings Inc* [2012] EWCA Civ 11; *Pipia v BGEO Group Ltd* [2020] EWHC 402 (Comm)). Ask how documents have in fact flowed within the group.
- **Service providers and former advisers.** Documents held by agents, outsourced IT providers, accountants and former solicitors are usually within the client's control through contract. Read the contract and write to them early.

Source architecture: never examine one location in isolation

Every piece of electronic evidence has a primary home and several secondary ones. When the primary source is unavailable, damaged, encrypted, deleted or outside your control, the same or corroborating evidence can usually be reached by another path. Build the alternatives into the plan at the start, because several of them (logs and backups especially) expire.

Alternative evidence paths

EVIDENCE	LOCAL DEVICE	CLOUD ACCOUNT	BACKUP	LOGS	COUNTERPART	DELETED BUT RECOVERABLE
Email	Y (cache)	Y	Y	Message trace, limited period	Y	Recoverable items, then backup
Chat and messaging	Y	Depends on app	Sometimes (device or cloud backup)	Limited	Y	Varies; device forensics
Files	Y	Y, with versions	Y	Access and sharing logs	If sent	Recycle bin, versions, carving
Location and movement	Y	Often	Sometimes	Wi-Fi, VPN, door access	n/a	Varies
User activity	Y (system artefacts)	Y	n/a	Y	n/a	Varies
Structured records	Rarely	Y	Y	Change and audit tables	Their ledger	Database logs

Fallback strategy. When the primary source fails, go first to the counterpart (the other end of the conversation always has a copy), then to logs (which prove that something existed and who touched it even when content is gone), then to backups, and only then to forensic recovery from the device, which is the slowest and least certain route.

PRACTICE POINT: NEWER SOURCES THAT ARE EASY TO MISS

- Links in chats and emails ("modern attachments") point to a live file; collect the file and the version that existed when the message was sent.
- Reactions, edits and deletions in chat platforms are recorded and can matter as much as the message.
- AI assistant prompts and outputs, meeting transcripts and automated summaries are documents.
- Shared and delegated mailboxes, distribution lists and team sites belong to no individual custodian and fall through custodian-based scoping unless listed separately.

Collection: method, metadata and chain of custody

Collection turns preserved data into evidence. The test is simple to state: could you prove to a sceptical judge that what you hold is a complete and unaltered copy of what was on the source, and show every hand it passed through?

Four principles

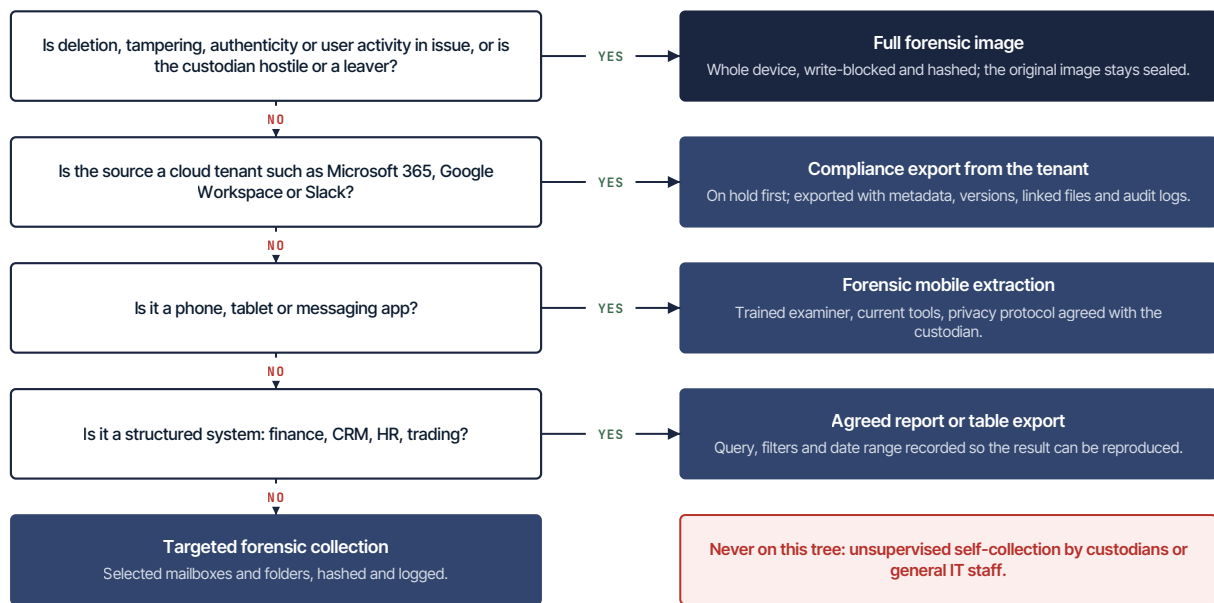
The long-standing principles for handling digital evidence, set out in the ACPO Good Practice Guide for Digital Evidence and reflected in ISO/IEC 27037, were written for criminal investigations but are the benchmark civil courts implicitly apply.

- | | |
|----|---|
| 01 | Do not change the data
No action taken should alter data that may later be relied on in court. |
| 02 | Competence
Where original data must be accessed, the person doing so must be competent and able to explain the relevance and implications of their actions. |
| 03 | Audit trail
A record of every process applied should be created and preserved, such that an independent third party could repeat the process and reach the same result. |
| 04 | Responsibility
The person in charge of the exercise has overall responsibility for ensuring that the law and these principles are followed. |

Choosing the method

METHOD	WHAT IT CAPTURES	USE WHEN
Full forensic image	Every sector of the storage device, including deleted files, system artefacts and unallocated space, verified by hash.	Deletion, tampering, authenticity, data theft or user activity is in issue; the custodian is hostile; the device may be the only source.
Targeted forensic collection	Selected folders, mailboxes or file types, copied with forensic tools that preserve metadata and log every file.	Ordinary commercial disclosure where content matters and device behaviour does not.
Cloud compliance export	Mailboxes, chats, sites and drives exported from the tenant with metadata, versions and audit logs.	Microsoft 365, Google Workspace, Slack and similar platforms. Needs appropriate licences and administrator rights.
Remote collection	As targeted collection, run over a secure connection with the custodian's cooperation.	Dispersed custodians, home workers, overseas offices.
Mobile extraction	Logical, file system or full file system extraction depending on handset, operating system and lock state.	Messaging apps, photos, location, call records. Always by a trained examiner.
Structured data export	Agreed reports or table extracts with a written description of the query and date range.	Finance, CRM, HR and trading systems.
Custodian self-collection	Whatever the custodian chooses to forward or copy, with altered metadata and no record of what was left behind.	Avoid. If unavoidable for low value items, supervise it, document it and tell the other side.

FIGURE 10 Choosing a collection method



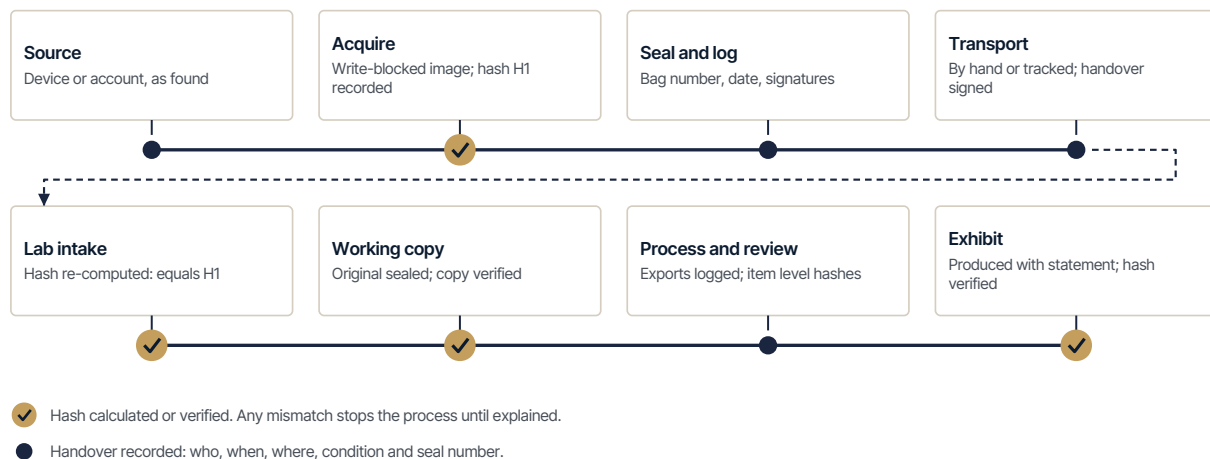
The more the dispute is about what happened on the device itself, the closer the method must be to a full forensic image. Custodian self-collection appears nowhere on the tree.

Metadata: what careless handling destroys

COMMON SHORTCUT	WHAT IS LOST OR ALTERED
Dragging files to a USB stick or shared folder	Created and accessed dates are reset; original path and ownership are lost; no record of what was not copied.
Forwarding emails to the solicitor	The original header, routing data, message identifier and thread position are replaced by those of the forward; attachments may be stripped.
Printing or saving to PDF	All file system and embedded metadata, tracked changes, comments, hidden rows and formulae.
Screenshots of chats	Message identifiers, exact timestamps and time zones, edit and deletion history, attachments, participant identifiers. Authenticity cannot be tested.
Opening files to "check" them	Last accessed dates and, in some applications, last modified dates and auto-saved content.
Exporting a chat with the app's own "export" function	Usually a text file without the underlying database, so deleted messages and metadata are unavailable.

Hashing and chain of custody

A hash value is a digital fingerprint calculated from the content of a file or an entire image. If a single bit changes, the hash changes. Hashes are calculated at acquisition and verified whenever the data is copied or loaded, which allows anyone to confirm later that the evidence is unchanged. MD5 and SHA-1 remain in common use for de-duplication and legacy compatibility; SHA-256 is preferred for integrity verification.

FIGURE 11 Chain of custody: from source to courtroom

Each handover is recorded and each copy is verified against the acquisition hash. A gap in the chain does not make evidence inadmissible in civil proceedings, but it hands the opponent an argument about weight.

CHAIN OF CUSTODY RECORD • EXHIBIT CFL/JS/01			SEALED
ITEM Dell Latitude 7440, serial ending 4KX9, 512 GB NVMe, BitLocker enabled (recovery key supplied by client IT)	ACQUIRED 14 Sep 2026 10:42 BST, client premises, by J. Smith (examiner), witnessed by client IT manager	METHOD Full physical image, write-blocked, E01 format, verified on completion	
VERIFICATION			
SHA-256 AT ACQUISITION 9f2c4a71e08b55d3...c41d7be2	SHA-256 AT LAB INTAKE 9f2c4a71e08b55d3...c41d7be2 MATCH	WORKING COPY Created 14 Sep 2026 16:05; original image sealed in evidence store, bag 0045519	
MOVEMENTS			
14 Sep 10:42	Acquired on site. Device returned to custodian's manager, receipt signed.		
14 Sep 15:30	Image drive delivered by hand to laboratory, logged into evidence store.		
15 Sep 09:10	Working copy released to processing. Targeted export of user profile to review platform.		

Illustrative record. Names, identifiers and hash values are fictitious.

Mobile devices

Phones hold the most candid evidence and are the hardest source to collect. What can be extracted depends on the handset model, operating system version, whether the passcode is known and whether the device has been unlocked since it was last switched on. Encrypted cloud backups and end to end encrypted messaging mean that the handset itself is often the only complete source. Practical rules: keep the device charged and do not let it update; record the passcode; disable disappearing messages; do not rely on screenshots or the app's own export; and have the extraction done by a trained examiner with current tools. The availability of some cloud encryption features in the UK has changed more than once since 2025, so check the position for the specific account at the time of collection.

Because phones mix private life with work, collection should be privacy-protective by design: an independent examiner, a written protocol agreed with the custodian, extraction of the whole device for integrity but export to the legal team of only the agreed apps, contacts, date ranges or search hits. It builds on the approach upheld in *Phones 4U*, where devices went to IT consultants bound by undertakings, and it answers most data protection and confidentiality objections before they are raised.

Privilege, confidentiality and data protection at collection

- **Collect wide, give access narrow.** It is usually cheaper and safer to collect complete mailboxes for Tier 1 custodians than to risk missing material, provided that access is restricted and culling happens before anyone reads the data.

- **Flag likely privilege early.** Ask custodians which lawyers they dealt with and feed names and domains into the privilege screen (Section 13).
- **Minimise lawfully.** Apply custodian, date and file type limits at the point of export where the platform allows. Record the lawful basis, use a processor agreement under UK GDPR Article 28 with the provider, and consider a data protection impact assessment for large or sensitive collections.
- **Keep data in the UK unless there is a reason and a lawful route to move it** (Section 16).

RED FLAG

"Our IT team has already pulled the emails." Ask immediately how, by whom, using what tool, with what search, and whether the originals are still on hold. An uncontrolled first collection should be treated as a pointer to the evidence, never as the evidence itself.

KEY POINTS

- Match the method to the issue: the more the device's own behaviour matters, the closer you need to be to a full forensic image.
- Hash at acquisition, verify at every copy, record every handover.
- Never let custodians collect their own documents unsupervised.



From data to disclosure

Six sections that follow the evidence from the processing engine to the trial bundle: reducing volume defensibly, designing searches that work, running review, using machine learning and generative AI, protecting privilege, and producing in a form the court expects.

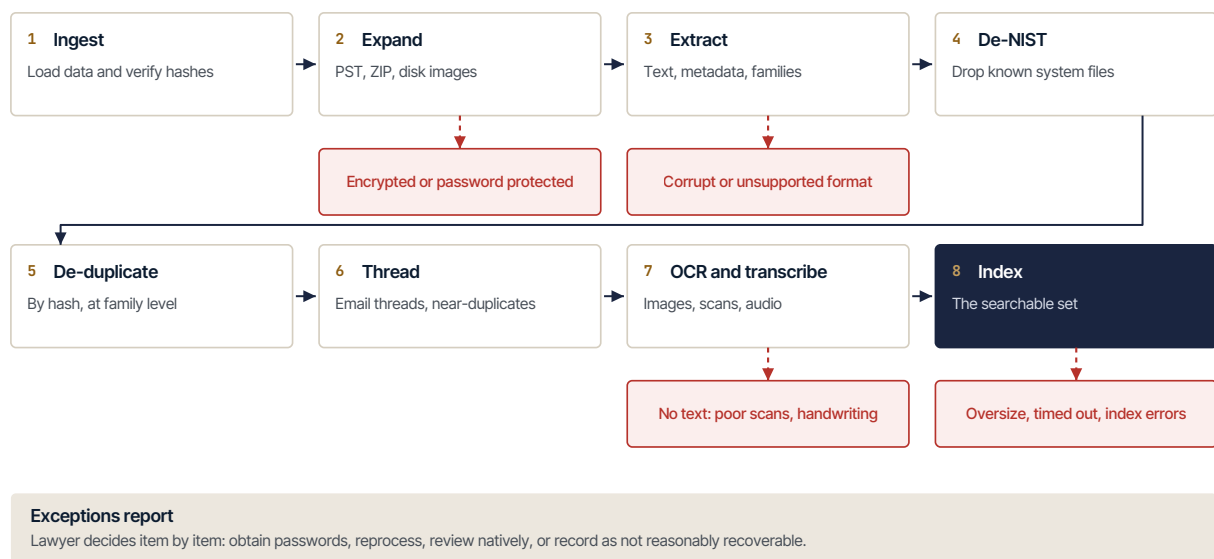
09	Processing and early case assessment	32
10	Search: keywords, analytics and defensibility	34
11	Document review	36
12	Technology assisted review and generative AI	38
13	Privilege, confidentiality and redaction	41
14	Production, inspection and presentation	44

Processing and early case assessment

Processing converts a heap of mailboxes, chats and disk images into a searchable, countable set. Early case assessment then uses that set to answer the questions that matter before serious money is spent: what have we got, what does it say, and what will it cost to review?

What processing does

FIGURE 12 The processing pipeline and its exceptions lane



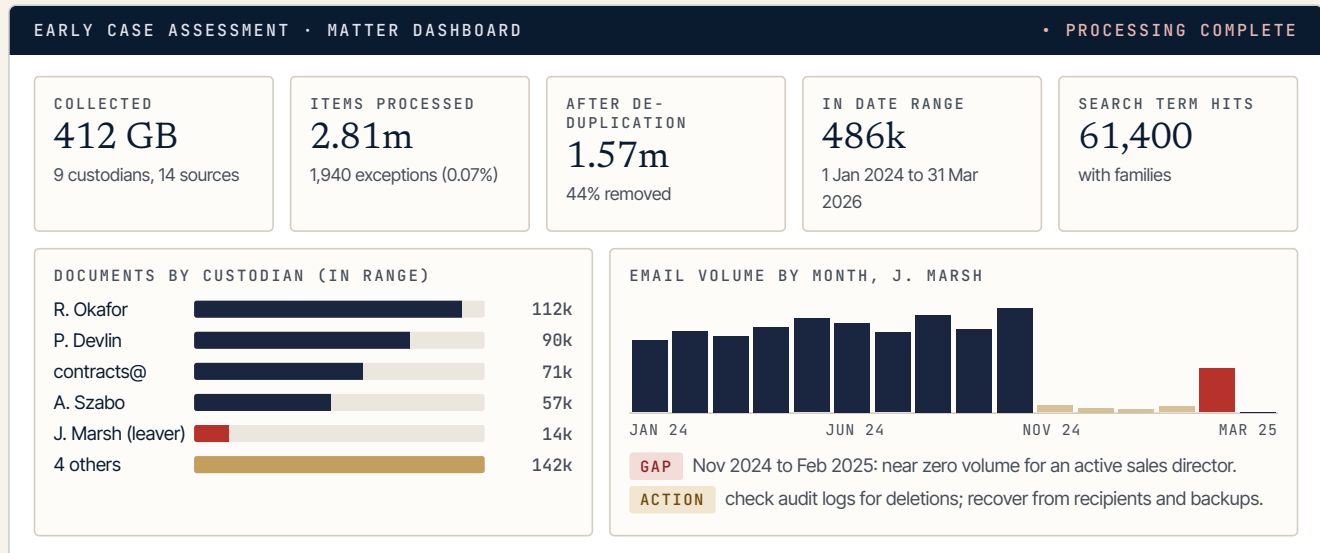
Everything that fails a step drops into the exceptions lane. An unread exceptions report is a list of documents nobody has searched.

Most of the pipeline is automatic, but several settings are legal decisions in disguise. They should be made by the supervising lawyer, recorded, and where appropriate agreed with the other side.

SETTING	THE DECISION	SENSIBLE DEFAULT
De-duplication and families	Remove duplicates within each custodian only, or across the whole data set? Are emails and attachments kept together?	Global, at family level, keeping a field that lists every custodian who held a copy. A hit on any family member brings the family.
Time zone	Which zone are dates normalised to? An email sent at 23:30 in New York is dated the next day in London.	One zone for the matter (often UTC or UK time), stated in the DRD and the production protocol.
Date filter	Which date field: sent, received, created, last modified? What about undated items?	Sent date for email; last modified for loose files; undated items retained.
System files and embedded objects	Remove program files using the NIST reference list (de-NISTing)? Extract logos embedded in emails as separate documents?	De-NIST disk images. Extract substantive embedded objects; suppress signature logos.
Exceptions	What happens to encrypted, corrupt or unsupported files?	Attempt passwords from custodians, reprocess, then list what remains and decide whether it matters.
Audio, video and images	Transcribe and OCR, or review natively?	OCR all image-only files; machine transcription for audio where the issues justify it, with human checking of anything relied on.

Early data assessment and early case assessment

The two phrases are often used as one, but they answer different questions. **Early data assessment** measures the data: volumes, custodians, date coverage, file types, languages and gaps. **Early case assessment** uses the data to assess the dispute: what the key documents say, how strong the case is, what it is worth and whether to settle. The first is a precondition for a sensible Disclosure Review Document. The second is often the best value work done in the whole matter, because it puts the documents that decide the case in front of the decision makers months before disclosure would.



Illustrative dashboard. The most valuable finding in early assessment is often an absence: a custodian, a month or a channel that should be there and is not.

What to measure, and what to do with it

MEASUREMENT	USE
Volume by custodian and source	Confirms the collection is complete; supports tiering decisions and the DRD.
Date coverage and gaps	Reveals missing periods, deletion and leavers' lost data while alternatives can still be found.
Top correspondents and domains	Finds unknown custodians, personal email use, lawyers (for the privilege screen) and third parties.
File types and languages	Identifies audio, images, foreign language and structured data that need special handling and budget.
Hit counts by search term	Evidence for negotiating terms with the opponent and for proportionality arguments (Section 10).
Sampled richness	The proportion of relevant documents in a random sample predicts review size and guides the choice of review technology.
Cost projection	Documents for review multiplied by an all-in cost per document, with a range. Feeds Precedent H and the DRD cost estimates.

PRACTICE POINT: ASSESSMENT IS A DATA MINIMISATION MEASURE

Culling by custodian, date, file type and tested search terms before human review is not only cheaper. It is how a disclosure exercise complies with the data minimisation principle in UK GDPR Article 5(1)(c): fewer people's personal data are read by fewer reviewers. Say so in the file.

Search: keywords, analytics and defensibility

A search is reasonable when it is designed from the issues, tested against the data, adjusted in the light of results and explained to the other side. It is not reasonable merely because a list of words was run.

Why keywords disappoint

Keyword searching feels precise and is not. People write in shorthand, nicknames, project codes and misspellings. They avoid the obvious word when the subject is sensitive. A classic study of lawyers searching a litigation database (Blair and Maron, 1985) found that the searchers believed they had found about three quarters of the relevant documents when they had found roughly one fifth. PD31B recognises the point, warning that keyword searches may yield both too much and too little. Keywords remain useful, particularly for culling and negotiated scope, but only when they are tested.

A defensible method

01 Start from the Issues for Disclosure

For each issue list the people, events, dates, products and concepts involved. Search design is issue by issue, as the Models are.

02 Harvest the language

Use custodian interviews and a first look at key documents to collect project names, abbreviations, nicknames, customer codes and the euphemisms people used.

03 Draft with proper syntax

Combine terms with proximity operators ("price w/10 increase"), wildcards and stemming. Avoid bare common words. Check how the platform treats punctuation, numbers and noise words.

04 Run a hit report

For every term: documents hit, documents with families, and unique hits (documents found by that term alone). Unique hits show what each term really contributes.

05 Sample

Review a random sample of each doubtful term's unique hits to estimate precision. Sample the null set (documents hit by no term) to estimate what is being missed.

06 Adjust and repeat

Narrow noisy terms, drop useless ones, add terms suggested by what the null set sample reveals.

07 Share and agree

Exchange proposed terms and hit reports with the opponent through the DRD. Record what is agreed and what is not.

Illustrative hit report after the first test run

TERM	DOCS HIT	WITH FAMILY	UNIQUE	SAMPLE PRECISION	DECISION
"Project Kestrel"	3,210	5,940	1,120	71%	Keep
margin	48,700	96,300	34,000	2%	Drop or narrow
(margin OR pric*) w/10 (Harlow OR tender)	4,480	8,150	3,100	38%	Keep
"off the record" OR "between us" OR "delete this"	390	610	240	44%	Keep (behavioural terms)

TERM	DOCS HIT	WITH FAMILY	UNIQUE	SAMPLE PRECISION	DECISION
CAD w/5 (copy OR download* OR export*)	1,870	2,400	960	17%	Narrow by date and custodian

CASE NOTE

Digicel (St Lucia) Ltd v Cable & Wireless plc [2008] EWHC 2522 (Ch). Whether a search was reasonable is a question for the court, not for the searching party alone. A party that chose its own keywords and left out backup tapes holding former employees' mailboxes was ordered to do more, and the parties were told to meet to discuss terms. The modern rules build that discussion into the DRD.

Voltaire Capital Holdings Ltd v Watson [2025] EWHC 1948 (Comm). Disagreements about scope are meant to be resolved quickly and cheaply at a Disclosure Guidance Hearing, with costs in the case. Here the hearing had grown into a contested application (two and a half hours, leading counsel, a 900 page bundle) and the court departed from the default: the unsuccessful party paid £63,267. Narrow the dispute with hit reports before you go to court.

Analytics that earn their keep

TOOL	WHAT IT DOES FOR YOU
Email threading	Groups messages into conversations and identifies the inclusive messages that contain the whole thread, often cutting email review by a third or more.
Near-duplicate detection	Groups drafts and versions so they are coded consistently and compared quickly.
Clustering and concept search	Groups documents by subject without keywords, exposing themes and vocabulary nobody thought to search for.
Communication maps	Shows who talked to whom, when and how much, which finds missing custodians and unusual channels.
Entity and pattern extraction	Pulls out names, account numbers, amounts and dates, and flags personal data for redaction planning.
Timelines, gap analysis and language detection	Plots activity against key events, makes deletions and silences visible, and routes foreign language material to the right reviewers.

Technical limits to keep in mind

- Text that was never extracted cannot be searched: image-only PDFs, photographs of documents, handwriting and poor scans need OCR, and OCR is imperfect.
- Audio and video are invisible to text search unless transcribed.
- Chat data is short, informal and full of emoji, reactions and in-jokes. Search it by participants and date as well as by words, and review it as conversations, not as single messages.
- Encrypted files appear in the exceptions report, not in the search results, and spreadsheets and databases hold meaning in structure and formulae that a keyword will not find.

KEY POINTS

- Test every term against the data and keep the hit reports.
- Sample the null set. It is the only way to know what the search is missing.
- Agree methodology through the DRD and record the agreement.

SECTION 11 • REVIEW — PD57AD 3.1(4), 3.1(6), 3.2(5)

Document review

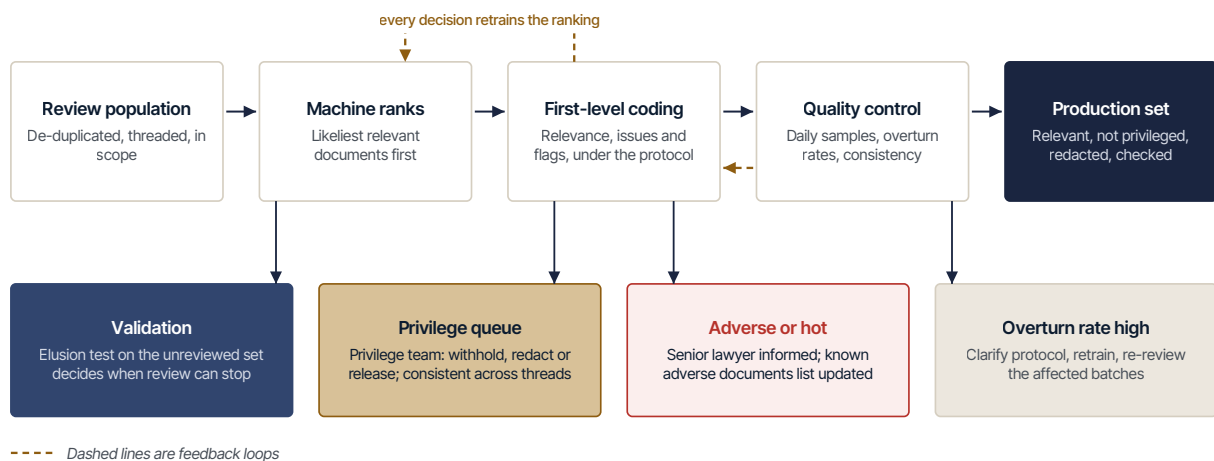
Review is where lawyers read documents and make the decisions the court relies on: relevant or not, to which issue, privileged or not, adverse or not. It is the most expensive stage and the one most exposed to human inconsistency, so it needs structure.

The review protocol

No review should start without a written protocol. It is the single most effective quality control, and it is the document you will want to have if the review is ever challenged. It should contain:

- a two page case summary: parties, chronology, the Issues for Disclosure and the Model ordered for each;
- a cast list with roles, nicknames and email addresses, including all lawyers (for privilege);
- coding definitions with examples of relevant, not relevant and borderline documents for each issue;
- the privilege rules for this matter and the escalation route (Section 13);
- what makes a document “hot” or a known adverse document, and who must be told;
- how to treat families, threads, duplicates, drafts and foreign language items;
- confidentiality and personal data flags that will drive redaction;
- technical issue tags (unreadable, password protected, needs native review);
- the quality control plan: sampling rates, overturn thresholds, feedback loops;
- a decision log, updated as questions arise, so that rulings are applied consistently.

FIGURE 13 Review workflow with quality control and escalation



Technology ranks the queue, people make the decisions, and quality control tests both. Privilege and adverse documents leave the main flow for senior decisions.

REVIEW PLATFORM • CODING PANEL

DOC ID ALD0048213 • THREAD 4 OF 7

DOCUMENT

From: R. Okafor **To:** P. Devlin **Sent:** 12 Feb 2025 17:48 UTC

Subject: RE: Harlow renewal, revised numbers

"Pete, before this goes to legal: the 2.5% we quoted them assumed the old volumes. If they see the internal sheet we have a problem on the rebate point. Call me, don't reply on here."

1 ATTACHMENT NEAR-DUPES 2 TAR RANK 0.94

RELEVANCE

RELEVANT NOT RELEVANT

ISSUES

1 DELIVERY 2 PRICING

3 CAD 4 QUANTUM

PRIVILEGE

NONE FULL PART QUERY

FLAGS

ADVERSE HOT

CONFIDENTIAL

PERSONAL DATA

REVIEWER NOTE

Adverse on Issue 2. "Before this goes to legal" is not a request for advice; not privileged. Escalated to supervising associate.

Illustrative coding panel. Fictitious parties and content.

Running the review

People

Train the team in person on the case, not only on the platform. Give them the pleadings summary and a set of pre-coded examples. Keep the team as small and stable as the timetable allows: consistency falls as headcount rises. Reviewers should be able to ask questions quickly and see the answers recorded in the decision log.

Order of work

Review whole threads and families together. Batch by custodian, cluster or machine ranking so that reviewers see related documents consecutively. Put the documents most likely to be relevant first (Section 12), so that the legal team learns the case early and the review can stop defensibly when little remains to be found.

Quality control

Second-review a random sample of each reviewer's work every day, more heavily in the first week. Track the overturn rate (the proportion of decisions changed) by reviewer and by tag. Re-train or reassign where it stays high. Run targeted checks as well: every document coded privileged, every document from a lawyer's domain coded not privileged, every "hot" document, and inconsistent coding across near-duplicates and within threads.

Known adverse documents

Under PD57AD a party must disclose known adverse documents whatever Model is ordered. A document becomes "known" when the relevant people in the organisation or its legal team become aware of it, and review is where that usually happens. The protocol must say what reviewers do when they see one, and the supervising lawyer must keep a list, because the Disclosure Certificate will confirm that the duty has been met.

RED FLAG

Relevance rates that differ sharply between reviewers, or that drift over time, mean the protocol is unclear or is being ignored. Stop, recalibrate and re-review the affected batches. It is far cheaper than explaining inconsistent disclosure to the court.

Do not over-disclose

Coding everything "relevant" to be safe is not safe. PD57AD paragraph 3.1(6) imposes a duty to use reasonable efforts to avoid providing documents that have no relevance to the Issues for Disclosure. Over-disclosure buries the other side and the court in noise, increases the risk of releasing privileged or confidential material, and invites costs sanctions.

KEY POINTS

- Write the protocol first, keep a decision log, and measure overturn rates daily.
- Give privilege and adverse documents their own escalation route.
- Small, stable, well briefed teams beat large ones.

Technology assisted review and generative AI

Machine learning has been an accepted part of English disclosure for a decade. Generative AI is now arriving in the same workflow. The legal question is the same for both: can you show that the process was reasonable, transparent and validated?

Three generations of technology

APPROACH	HOW IT WORKS	BEST FOR
Predictive coding (TAR 1.0)	Senior lawyers code a seed set; the system learns, scores every document once, and a cut-off score divides the set into review and no review. A separate control set measures performance.	Very large, stable data sets with an early fixed scope. Now largely superseded.
Continuous active learning (TAR 2.0, CAL)	The model learns from every coding decision and continually re-ranks the unreviewed documents so that the likeliest relevant ones are served next. Review stops when validation shows little of value remains.	Most disclosure exercises above a few tens of thousands of documents, including rolling collections.
Generative AI review	A large language model is given the issues and coding criteria as a prompt and returns a classification with a written rationale for each document. Often combined with CAL and human checking.	First pass relevance and issue coding, summarising long documents, translation, chronology building and privilege screening support.

The English authorities

CASE NOTES

Pyrrho Investments Ltd v MWB Property Ltd [2016] EWHC 256 (Ch). The first English judgment to approve predictive coding. Master Matthews gave ten reasons at paragraph 33, including experience in other jurisdictions, greater consistency than manual review, the absence of any rule against it, the size of the data set (over three million documents), cost, and the parties’ agreement.

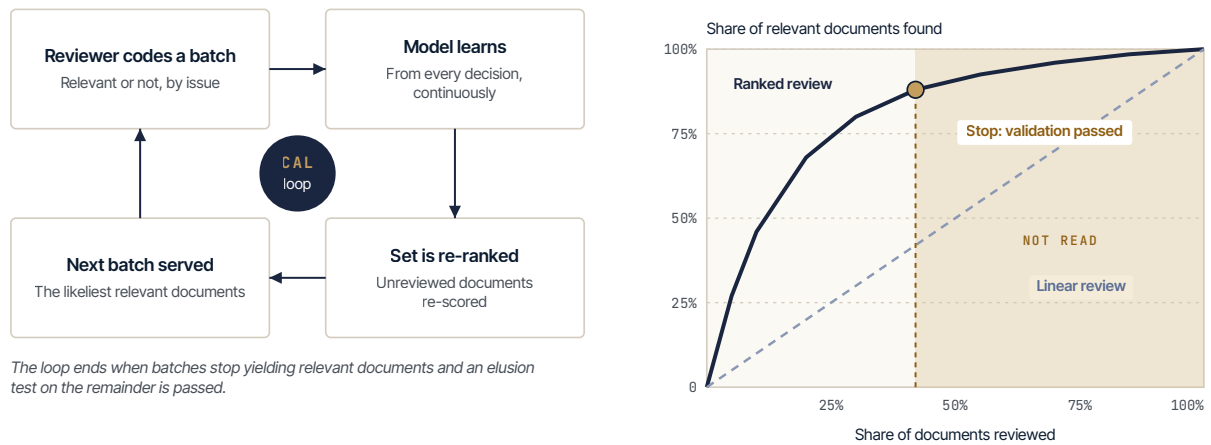
Brown v BCA Trading Ltd [2016] EWHC 1464 (Ch). Predictive coding was ordered over the other side’s objection, largely on cost: an estimated £132,000 against £250,000 to £338,000 for a keyword approach.

Triumph Controls UK Ltd v Primus International Holding Co [2018] EWHC 176 (TCC). The cautionary tale. One party used computer assisted review and sampling to cut down its review without agreeing the approach with the other side. The court found the process neither transparent nor independently verifiable and ordered a manual review of a 25% sample of some 220,000 documents.

The rules now assume the technology will be considered. Legal representatives must cooperate “including through the use of technology” (PD57AD paragraph 3.2(3)); the parties must discuss software and analytical tools including technology assisted review (paragraph 9.6(3)); and Section 2 of the DRD asks each party, particularly where the review universe exceeds 50,000 documents, to explain why such tools will not be used if that is the proposal. The judicial AI guidance of October 2025 describes technology assisted review as now part of the landscape of electronic disclosure. It is a threshold for explanation, not a mandate: in the 2026 working group survey two thirds of respondents opposed mandatory technology thresholds.

How ranked review works

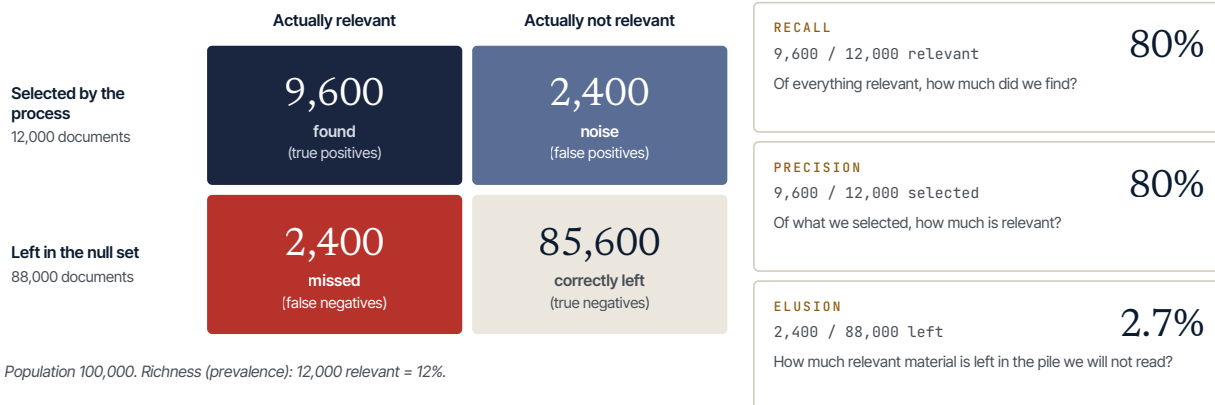
FIGURE 14 How continuous active learning finds the relevant documents first



Illustrative gain curve. With ranking, most relevant documents are found in the first part of the review; the decision to stop is then taken on evidence, by validation, and not by exhaustion of the budget.

Validation: the numbers that make it defensible

FIGURE 15 Recall, precision and elusion explained



Recall answers "how much of what matters did we find?" Elusion answers "how much is left in the pile we are not going to read?" Both are estimated from random samples.

RANDOM SAMPLE SIZE	MARGIN OF ERROR	TYPICAL USE
385 documents	about ±5%	Quick richness estimate; testing a single search term.
1,537 documents	about ±2.5%	Elusion test or control set for a standard matter.
2,401 documents	about ±2%	High value or contested validation.

At 95% confidence, large population, worst case proportion. No English rule prescribes a recall figure; parties commonly negotiate 70% to 80% with an agreed elusion test. What matters is that target, method and result are agreed or at least disclosed.

Generative AI in disclosure

Large language models can read a document against a written description of the issues and return a decision with reasons. Used well, that is fast, consistent and auditable, because the rationale is recorded for every document. Used carelessly, it introduces new risks.

RISK	CONTROL
Confidentiality and privilege	Use only enterprise deployments with contractual commitments that client data is not used for training, with UK or agreed data residency and access logging. Never paste disclosure material into consumer tools.
Plausible but wrong reasoning	Treat the output as a first pass. Validate with the same statistics as any other review (precision, recall, elusion) and have lawyers check samples of both positive and negative calls.
Prompt sensitivity and reproducibility	Draft prompts from the Issues for Disclosure, test them on a coded sample, version control every change and keep the prompt history. Record the model and version: rerunning the same prompt months later may give different answers.
Accountability	The lawyer remains responsible. In <i>R (Ayinde) v London Borough of Haringey</i> [2025] EWHC 1383 (Admin) the Divisional Court confirmed that lawyers must verify AI output against authoritative sources, with sanctions up to contempt for those who do not.
Data protection	Treat the AI provider as a processor or sub-processor, update the processing agreement and the impact assessment, and consider the automated decision-making rules as amended by the Data (Use and Access) Act 2025 where individuals are affected.

The most useful current guidance is the ILTA Generative AI Best Practice Guide (final version 30 September 2025), discussed on the Law Society's website, which recommends agreeing the scope and parameters of generative AI use with the opponent early, keeping review human-led, structured testing and validation, prompt management with an audit trail, and clear practitioner accountability. The Civil Justice Council's working group on AI in preparing court documents, in its 2026 interim report, saw no pressing case for disclosure lists to address AI use specifically, which leaves the matter to the DRD, cooperation and the general duties.

What to agree with the other side

- | | |
|---|---|
| <ul style="list-style-type: none"> ☐ The tool and the approach (CAL, generative AI, or both) and the document population it will be applied to. ☐ Any culling before the tool is applied (custodians, dates, search terms). ☐ Who trains or prompts the system and how privilege is protected during training. ☐ The validation method: sample sizes, target recall or elusion rate, and who reviews the samples. | <ul style="list-style-type: none"> ☐ What will be shared: metrics always; seed or validation documents only by agreement and never privileged material. ☐ What happens if validation fails: further training rounds, revised prompts, and how quickly the other side is told. The duty to cooperate means difficulties are raised promptly, not discovered later. ☐ Treatment of documents the tool cannot read: images, audio, spreadsheets with little text, very short messages. |
|---|---|

US COMPARISON

US courts have accepted technology assisted review since *Da Silva Moore v Publicis Groupe*, 287 F.R.D. 182 (S.D.N.Y. 2012). The validation protocol ordered in *In re Broiler Chicken Antitrust Litigation* (N.D. Ill. 2018) is a widely borrowed model and applies whether review is by machine learning, keywords or linear review. Commentary on recent decisions suggests US courts are starting to treat generative AI review as a species of technology assisted review.

KEY POINTS

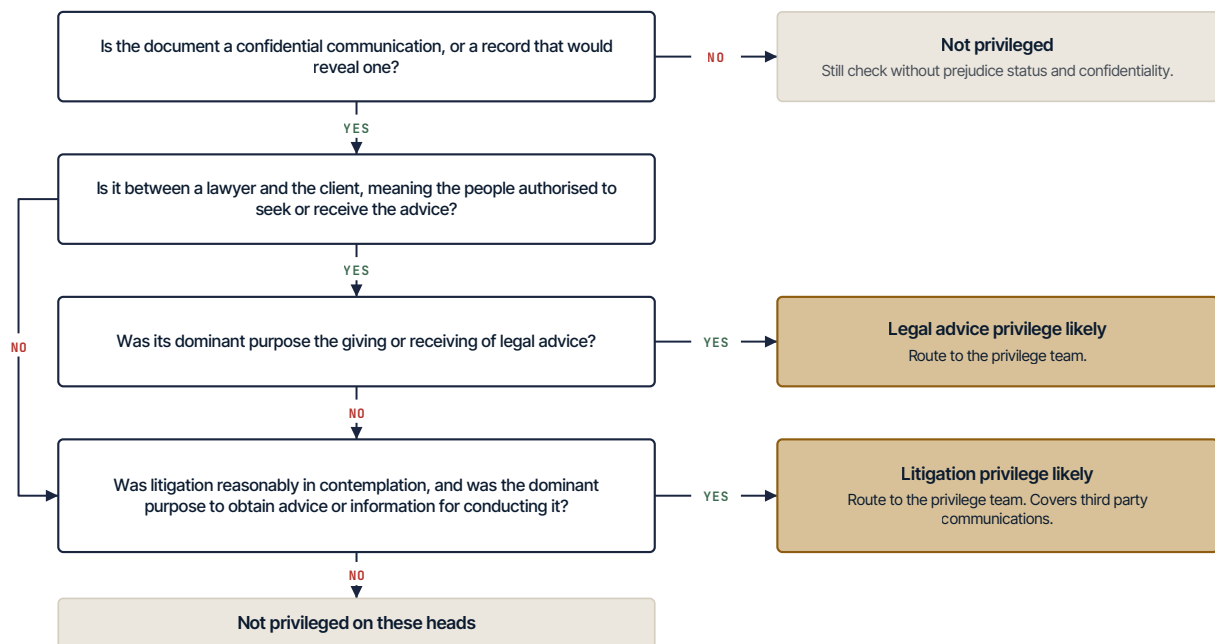
- Above 50,000 documents, be ready to explain why review technology is not being used.
- Transparency is the lesson of *Triumph Controls*: agree the method, or at least disclose it.
- Generative AI is validated like any other review method, and the lawyer remains accountable for the result.

Privilege, confidentiality and redaction

Privilege is the one category of relevant document a party is entitled to withhold, and the one mistake in disclosure that cannot be fully undone. The law is English; the risk is operational.

The English law of privilege in one page

FIGURE 16 Is this document privileged? A first-pass decision tree



Then ask: has privilege been lost (waiver, loss of confidence, iniquity)? Is only part privileged, so redaction is the answer?

A screening aid for reviewers, not a substitute for a lawyer's decision. Anything that reaches a brass box goes to the privilege team.

HEAD	ESSENTIALS
Legal advice privilege	Confidential communications between lawyer and client for the dominant purpose of giving or receiving legal advice (<i>R (Jet2.com Ltd) v Civil Aviation Authority</i> [2020] EWCA Civ 35). "Client" means those authorised to seek and receive the advice, not every employee (<i>Three Rivers (No 5)</i> , by which the Court of Appeal held itself bound in <i>SFO v ENRC</i>). Includes in-house and foreign lawyers; excludes accountants and other non-lawyers giving legal advice (<i>R (Prudential plc) v Special Commissioner of Income Tax</i> [2013] UKSC 1).
Litigation privilege	Confidential communications between lawyer or client and third parties, or documents created, for the dominant purpose of litigation that is in reasonable contemplation. In <i>SFO v ENRC</i> [2018] EWCA Civ 2006 the Court of Appeal allowed the company's appeal and upheld litigation privilege over internal investigation material. The purpose must be obtaining information or advice for the conduct of the litigation (<i>WH Holding Ltd v E20 Stadium LLP</i> [2018] EWCA Civ 2652).
Without prejudice	Genuine settlement communications generally cannot be put before the court. The other party to them already has them, so the practical tasks are to tag them, keep them out of bundles and protect them from third parties and co-defendants.
Common interest and joint privilege	Sharing privileged material with a party who has a common interest (insurer, group company, co-defendant) does not necessarily waive privilege. Record the basis before sharing.

HEAD	ESSENTIALS
Loss of privilege	Waiver by deployment or by loss of confidentiality; the iniquity exception where the communication furthers wrongdoing (<i>Al Sadeq v Dechert LLP</i> [2024] EWCA Civ 28).
Which law applies?	An English court applies English privilege rules to documents wherever they were created (<i>Re RBS Rights Issue Litigation</i> [2016] EWHC 3161 (Ch)). A document privileged in New York may not be privileged in London, and the reverse.

A privilege workflow that holds up

- 01 **Build the screen**
List every lawyer and law firm (names, email addresses, domains), plus terms such as “privileged”, “legal advice” and “without prejudice”. Documents hitting the screen are routed to a privilege queue before anyone else sees them.
- 02 **Use a dedicated privilege team**
First level reviewers flag; experienced lawyers decide. PD57AD paragraph 3.2(5) makes the legal representative personally responsible for being satisfied that privilege claims are properly made.
- 03 **Decide at the right level**
Assess each email in a thread and each attachment separately. A privileged email does not make its attachment privileged, and forwarding advice internally does not necessarily lose privilege.
- 04 **Redact where only part is privileged**
Produce the rest. PD57AD paragraph 16 requires the redaction to be explained and confirmed as reviewed by a legal representative.
- 05 **Enforce consistency**
Run duplicate, near-duplicate and thread consistency reports before production. Most inadvertent disclosures are a copy of a withheld document that was coded differently elsewhere.
- 06 **Describe what is withheld**
English practice permits privileged documents to be described by class (PD57AD paragraph 14.1), but be ready to justify each class if the claim is challenged (by application under PD57AD paragraph 14.2, or under CPR 31.19 in Part 31 cases).

When it goes wrong: inadvertent disclosure

If a privileged document is inspected by mistake, the receiving party may use it only with the court’s permission (CPR 31.20; PD57AD paragraph 19.1). A lawyer who realises that a document has been disclosed by mistake should stop reading, notify the other side promptly, and return or destroy it (paragraph 19.2); a solicitor’s duty to share material information with the client does not extend to a privileged document known only because it was mistakenly disclosed (SRA Code, paragraph 6.4(d)). The court asks whether the mistake would have been obvious to a reasonable solicitor. In *Atlantisrealm Ltd v Intelligent Land Investments (Renewable Energy) Ltd* [2017] EWCA Civ 1029 the Court of Appeal granted relief where a junior reviewer had not noticed the mistake but a more senior lawyer did.

US COMPARISON

US practice manages the same risk by order. A Rule 502(d) order, obtained at the outset, provides that disclosure in the litigation is not a waiver in that or any other federal or state proceeding; Rule 26(b)(5)(B) then provides the clawback mechanism. There is no direct English equivalent, so in cross-border matters obtain the US order and also agree a written clawback protocol for the English proceedings. US attorney-client privilege treats corporate employees more generously than *Three Rivers (No 5)*, and the work product doctrine is not identical to litigation privilege: review teams working on both sides of the Atlantic need two sets of privilege instructions.

Confidentiality is not privilege

Confidential documents must be disclosed if relevant. Protection comes from the restriction on collateral use (CPR 31.22), from redaction of material that is both irrelevant and confidential (PD57AD paragraph 16.1), and, for commercially sensitive material, from a confidentiality ring or club limiting who on the receiving side may see it (paragraph 15). Personal data is treated the same way: relevant personal data is disclosed; irrelevant personal data may be redacted if it is confidential. Data protection law does not provide a free-standing right to withhold relevant documents (Section 17).

Redaction that actually redacts

- ☐ Redact on an image or PDF copy with a tool that removes the underlying text, then re-run OCR on the redacted image. A black box drawn over live text can be copied out by anyone.
- ☐ Remove or regenerate extracted text and metadata fields (subject, file name, author) that repeat the redacted content.
- ☐ Spreadsheets and other native files cannot be safely redacted in image form without losing function. Agree a method: a redacted native copy with cells cleared and a log, or an image with the native withheld.
- ☐ Label each redaction with its basis ("Privileged", "Irrelevant and confidential") so the other side and the court can follow it.
- ☐ Quality-control every redacted document before production, and search the production set for terms that should have been removed.

KEY POINTS

- English privilege is narrower than many clients and US colleagues expect, especially on who is the "client".
- Consistency checks across duplicates and threads prevent most inadvertent disclosures.
- Redaction is a technical process with known failure modes. Test it.

Production, inspection and presentation

Production is the moment the work becomes visible to the other side and the court. A clean, well documented production builds credibility. A chaotic one invites applications.

What is delivered

DELIVERABLE	NOTES
Disclosure Certificate (PD57AD) or disclosure statement (CPR 31.10)	Signed by the party. Describes the search, confirms the duties have been understood and met, and confirms known adverse documents have been disclosed. A false certificate is a contempt.
List of documents	The Extended Disclosure List of Documents under PD57AD paragraph 12, or form N265 under Part 31. For electronic disclosure this is normally an export of agreed fields, not a typed list.
The documents	Electronic documents in native format preserving metadata (PD57AD paragraph 13.1; PD31B paragraph 33), with searchable text. Redacted documents as images with fresh OCR.
Load file	A data file linking each document to its metadata, text and family, so the receiving platform can load the set without manual work.
Covering letter	Volumes, date ranges, custodians, numbering ranges, what is withheld and why, known gaps and how they are being addressed.

Agree the production protocol before anyone produces

ITEM	WHAT TO AGREE
Numbering	Prefix per party, document level numbering, how families are numbered, no reuse of numbers.
Format	Natives for all, or natives for spreadsheets, media and presentations with images for the rest. Image format and resolution. Chat data as conversations by channel and day, not one message per document.
Metadata fields	At least: document ID, family and parent ID, custodian and all custodians, from, to, cc, bcc, subject, sent and received dates, file name, file path, created and modified dates, author, file type, hash, time zone, redaction flag, confidentiality designation.
Time zone and date format	One zone for the matter; day-month-year to avoid transatlantic ambiguity.
De-duplication and threading	Whether duplicates were suppressed globally and whether only inclusive emails are produced. If so, all-custodian and thread fields must be supplied.
Transmission	Encrypted transfer or encrypted media, password sent separately, receipt acknowledged.
Replacement and clawback	How corrected or clawed back documents are handled and numbered.

Before it leaves: the pre-production check

- ☐ Counts reconcile: documents coded for production equal documents in the set, families complete.
- ☐ Nothing coded privileged or “query” is in the set; privilege screen terms re-run across the production.
- ☐ Redactions burned in and text regenerated; spot check by opening files.
- ☐ Numbering continuous with no gaps or overlaps.
- ☐ Metadata fields populated and dates in the agreed zone.
- ☐ Natives open; password protected files dealt with.
- ☐ Confidentiality designations applied.
- ☐ The known adverse documents list has been cross-checked against the set.
- ☐ A second person has signed off the production log.

Receiving the other side's disclosure

Intake is a forensic exercise in its own right. Load the production, then test it against what you were promised in the DRD. Look for custodians with implausibly low volumes, months with no email, channels that were agreed but are absent, missing attachments, metadata fields left blank, documents referred to in other documents but not produced, and redactions without explanation. Put the results in a gaps letter that is specific about what is missing and why you believe it exists. Specificity is what persuades a court under PD57AD paragraphs 17 and 18 or CPR 31.12; general complaints do not.

PRACTICE POINT

Documents disclosed to you may be used only for the purpose of the proceedings in which they were disclosed, until they are read or referred to in open court, or the court gives permission, or the disclosing party and the person to whom the document belongs agree (CPR 31.22). Brief the client and any experts on this before giving them access, particularly where related proceedings or regulatory complaints are in prospect.

From disclosure to the courtroom

Authenticity

A party is deemed to admit the authenticity of a document disclosed to it unless it serves a notice requiring the document to be proved at trial (CPR 32.19). If you doubt a document, whether a convenient email that surfaced late, an edited PDF, a screenshot of a chat or a contract with a suspicious signature page, serve the notice in time and ask for the native file with its metadata. That is the point at which a digital forensic expert should be instructed (Section 24).

Bundles

The General Guidance on Electronic Court Bundles requires bundles in PDF format, text searchable by OCR, with computer generated pagination that matches the PDF page numbers, bookmarks for each document and a hyperlinked index, at a resolution of no more than 300 dpi. Spreadsheets, audio, video and chat exports that lose meaning when flattened to PDF should be made available natively by agreement with the court. Present chat messages as conversations with participants, dates and times in the agreed zone.

Expert evidence

Where the integrity, origin or handling of electronic evidence is disputed, the court's permission is needed for expert evidence under CPR Part 35. The expert's overriding duty is to the court. Raise the need at the case management conference, define the questions narrowly, and consider whether a single joint expert or a joint inspection protocol would resolve the point at lower cost.

Closing the matter: disposal

At the end of the proceedings, including appeals and any related claims, release the legal hold, return or destroy the other side's disclosure in accordance with any order or agreement, archive what professional rules and insurers require, and have the provider delete hosted data and certify that it has done so. Hosting charges and data protection risk both continue until someone decides to stop them.

KEY POINTS

- Agree the production protocol early: numbering, format, fields, time zone.
- Check every production twice, once before it leaves and once when the other side's arrives.
- Challenge authenticity in time under CPR 32.19 and ask for natives.

IV

PART FOUR

Special situations

Evidence held by someone else, data that has to cross a border, personal data at every turn, a budget to defend, a provider to choose, and forums that do not follow the High Court's rules.

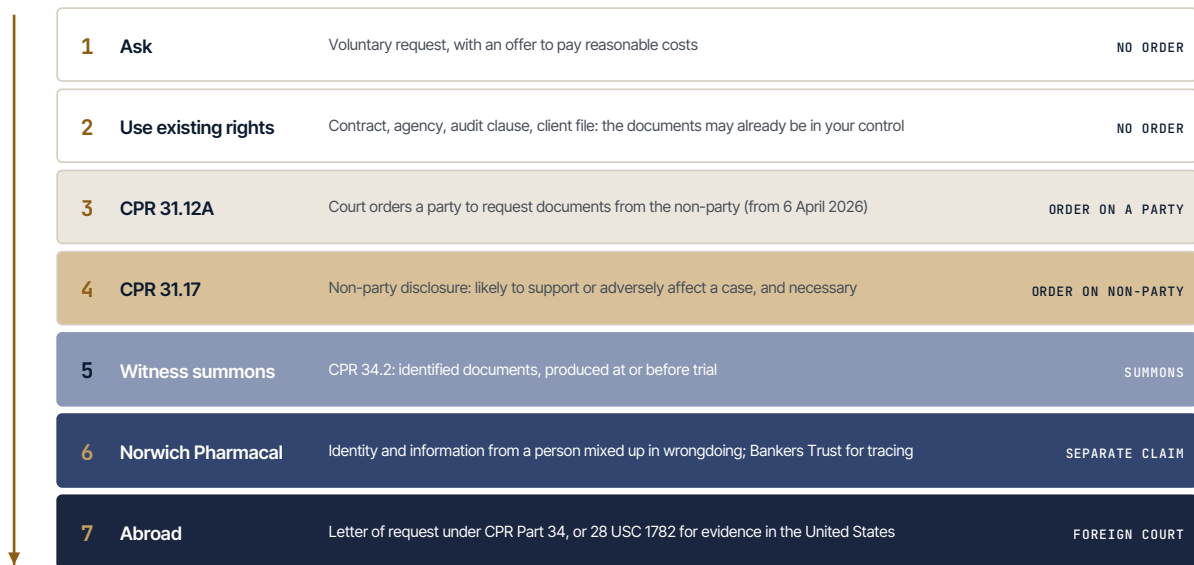
15	Documents held by non-parties	47
16	Cross-border matters: US discovery meets UK data	50
17	Data protection in disclosure	52
18	Costs and proportionality	54
19	Choosing technology and providers	56
20	Beyond the High Court: other forums and jurisdictions	57

Documents held by non-parties

In the United States a lawyer signs a subpoena and a stranger to the case must respond. England has no equivalent. A non-party can be made to produce documents only by court order, and the routes are narrower, slower and paid for by the applicant.

The routes

FIGURE 17 Routes to documents held by someone who is not a party



Cost, time and court involvement increase down the ladder

Work down the ladder. The cheapest routes are at the top, and the court will ask whether you tried them before applying.

ROUTE	TEST AND SCOPE	PRACTICAL NOTES
Ask	No test. Many banks, platforms and former advisers will help a customer or client on request, or will confirm what they hold.	Always first. Offer to pay reasonable costs and to narrow by date and subject.
Contractual or statutory right	Audit clauses, agency, rights to the client file, shareholder or director information rights.	Such documents may already be within your client's control (CPR 31.8) and therefore disclosable by it.
CPR 31.12A (from 6 April 2026)	The court may order a party to request any person to produce documents that may support or adversely affect a party's case. Mirrored by PD57AD paragraph 18.5.	Introduced after <i>McLaren Indy LLC v Alpa Racing USA LLC</i> [2025] EWHC 1825 (Comm) exposed the absence of such a power. It does not compel the non-party, but it removes a party's ability to refuse to ask. Useful for group companies, agents and friendly third parties.
CPR 31.17 non-party disclosure	Documents likely to support the applicant's case or adversely affect another party's, and disclosure necessary to dispose fairly of the claim or to save costs. The order must specify the documents or classes.	Only after proceedings have started. "Likely" means "may well". Classes must be tightly drawn; a fishing request fails. The applicant normally pays the respondent's costs of the application and of compliance (CPR 46.1).

ROUTE	TEST AND SCOPE	PRACTICAL NOTES
Witness summons (CPR 34.2)	Requires a witness to produce specified documents at trial or on a date fixed by the court.	For identified documents, not classes. Useful close to trial.
Pre-action disclosure (CPR 31.16)	Against a likely party only, where the documents would fall within standard disclosure and early disclosure is desirable to dispose fairly of the anticipated proceedings, assist resolution without proceedings, or save costs.	Not a route to strangers. Costs usually fall on the applicant.
Norwich Pharmacal order	Against a person mixed up, even innocently, in wrongdoing, where disclosure is necessary to enable action against the wrongdoer. Typically identities, account details and logs.	The main route to internet platforms, banks and telecoms providers before a claim can be framed. <i>Bankers Trust</i> orders serve a similar purpose in tracing assets.
Data subject access request	An individual's right to their own personal data (UK GDPR Article 15).	Limited to personal data, subject to exemptions and to redaction of third party information, but motive is irrelevant (<i>Dawson-Damer v Taylor Wessing LLP</i> [2017] EWCA Civ 74). See Section 17.
Abroad	Letter of request under CPR Part 34, or an application in the foreign court.	For US-held evidence, 28 U.S.C. section 1782 is usually faster and broader (Section 16).

Drafting a CPR 31.17 application that succeeds

- **Show you asked first**, and exhibit the correspondence.
- **Define documents by reference to the pleaded issues**, with custodians, date ranges and document types. "All documents relating to" is an invitation to refuse.
- **Explain necessity**: why the parties' own disclosure cannot supply the evidence, and what difference the documents will make.
- **Deal with confidentiality and personal data** in the draft order: confidentiality ring, redaction of irrelevant third party data, restricted use.
- **Offer a workable method**: agreed search terms, a provider to run them, a sensible timetable, and an undertaking on costs.

If your client is the non-party

Receiving a request or application in someone else's litigation is an unwelcome cost, but ignoring it is worse. A structured response protects the client and usually reduces the burden.

- 01 Preserve first**
Once on notice, put the relevant material on hold. Deleting it now would be very hard to explain.
- 02 Work out what you hold and whose it is**
Identify systems, volumes and whether the material includes other people's confidential information, personal data or privileged documents (your client's or a customer's).
- 03 Check duties to others**
Contractual confidentiality, banking or professional confidence, regulatory restrictions and data protection may mean you should not hand documents over without an order, even if willing.
- 04 Negotiate scope and cost**
Propose narrower custodians, dates and terms; ask for costs on the CPR 46.1 footing, including the cost of review and any provider.

05 Prefer a consent order

An order gives the client a lawful basis for disclosure, records the protections, and fixes the costs entitlement.

06 Review and produce properly

Review for privilege and third party confidentiality, produce securely with a list, and keep a record of what was given.

US COMPARISON: THE RULE 45 SUBPOENA

A subpoena is issued by an attorney as an officer of the court and served on the non-party. Written objections must be served before the earlier of the time for compliance or 14 days after service (Rule 45(d)(2)(B)); the issuing party must take reasonable steps to avoid undue burden or expense (45(d)(1)); the court must quash or modify a subpoena that allows no reasonable time, exceeds the geographical limits, requires privileged matter or imposes undue burden (45(d)(3)); and an order compelling production must protect a non-party from significant expense. A UK company served with a US subpoena through a US affiliate should take US advice immediately on whether it is validly served and enforceable, and UK advice on data protection and confidentiality before anything leaves the country (Section 16).

KEY POINTS

- There is no English subpoena. Every compulsory route needs a court order and a tightly specified request.
- CPR 31.12A is new and useful: the court can now order a party to ask.
- A non-party should preserve, scope, protect third party rights and recover its costs.

Cross-border matters: US discovery meets UK data

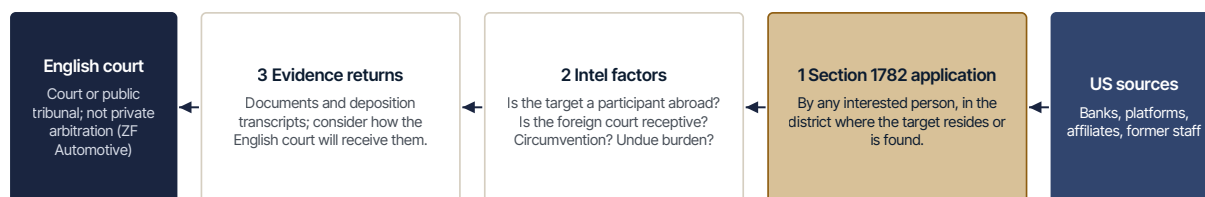
The most common cross-border problem on a London desk is a US court wanting documents that sit in the United Kingdom. The second is an English litigant who needs evidence from the United States. The routes, and the friction, are different in each direction.

FIGURE 18 Evidence across the Atlantic: the routes in each direction

WESTBOUND: UK DOCUMENTS FOR A US COURT



EASTBOUND: US EVIDENCE FOR ENGLISH PROCEEDINGS



Criminal and regulatory channels (mutual legal assistance, the UK-US Data Access Agreement) are separate and not shown.

Westbound data must pass two gates: a procedural route the English court will recognise, and a lawful transfer mechanism under UK data protection law. Eastbound, section 1782 offers English litigants something English procedure does not.

Westbound: US proceedings, UK documents

Where the UK entity is a party to the US case

A party to US litigation is subject to the Federal Rules directly, wherever its documents are. The US Supreme Court held in *Société Nationale Industrielle Aérospatiale v US District Court*, 482 U.S. 522 (1987), that the Hague Evidence Convention is neither exclusive nor a mandatory first resort; US courts weigh comity factors including the importance and specificity of the request, where the information originated, alternative means of obtaining it and the competing national interests. In practice UK data protection law is treated as a constraint to be managed, not a shield. The task is to comply with the US order in a way that is lawful in the UK.

Where the UK holder is not a party

A US court has no direct power over a UK non-party. The route is a letter of request under the Hague Evidence Convention, given effect in England by the Evidence (Proceedings in Other Jurisdictions) Act 1975 and CPR 34.16 to 34.21. Two limits matter. The United Kingdom made a declaration under Article 23 of the Convention that it will not execute letters of request issued for the purpose of obtaining pre-trial discovery of documents. And section 2(4) of the 1975 Act prevents an order requiring a person to state what documents they hold or to produce anything other than "particular documents specified in the order". Requests framed in US style ("all documents concerning") are refused or cut down (*Rio Tinto Zinc Corp v Westinghouse Electric Corp* [1978] AC 547). Requests for identified documents and for oral examination of named witnesses on defined topics succeed regularly. The Protection of Trading Interests Act 1980 also allows the Secretary of State to prohibit compliance with overseas demands that infringe UK sovereignty, a power rarely used.

The data protection gate

Whatever the procedural route, sending personal data to the United States is a restricted transfer under Chapter V of the UK GDPR. The UK GDPR contains no equivalent of Article 48 of the EU GDPR (it was omitted at the end of the Brexit transition period), so a foreign court order neither authorises nor blocks a transfer by its own force. The transfer needs one of the following.

MECHANISM	WHEN IT WORKS
UK-US data bridge	In force since 12 October 2023. Covers only US recipients certified to the UK Extension of the EU-US Data Privacy Framework. Many law firms, courts and opposing parties are not certified, so it rarely covers the whole chain.
International Data Transfer Agreement or Addendum	Contractual safeguards with the US recipient (for example US counsel or a US hosting provider), supported by a transfer risk assessment against the statutory data protection test.
Article 49(1)(e): legal claims	Transfer “necessary for the establishment, exercise or defence of legal claims”. ICO guidance updated in January 2026 stresses that the transfer must be necessary and proportionate and that the exception requires actual or genuinely prospective proceedings, not a mere possibility.

PRACTICE POINT: MINIMISE IN THE UK, THEN TRANSFER

The approach that satisfies both courts is to collect, process, search and review in the United Kingdom, and to transfer only the documents that are responsive. Redact or pseudonymise irrelevant personal data before transfer, obtain a US protective order restricting use and onward disclosure, designate sensitive material for attorneys’ eyes only, and keep a written record of the necessity assessment. US judges are generally receptive to a documented, good faith protocol of this kind; they are unreceptive to blanket refusals.

Eastbound: English proceedings, US evidence

Under 28 U.S.C. section 1782 a US district court may order a person who resides or is found in its district to give testimony or produce documents for use in a proceeding before a foreign or international tribunal, on the application of any interested person. The Supreme Court set out the discretionary factors in *Intel Corp v Advanced Micro Devices Inc*, 542 U.S. 241 (2004): whether the target is a participant in the foreign proceeding, the nature of the tribunal and its receptivity to US assistance, whether the request circumvents foreign proof gathering restrictions, and whether it is unduly intrusive or burdensome. The foreign proceeding need only be within reasonable contemplation and the material need not be discoverable under English rules. Section 1782 is not available in aid of private commercial arbitration (*ZF Automotive US Inc v Luxshare Ltd*, 596 U.S. 619 (2022)).

For English litigants this is a powerful tool: it can reach US banks, technology companies, former employees and affiliates, and it brings US style document requests and depositions. Consider it early and take US advice on venue and timing.

Working with US counsel: a short protocol

- ☐ Issue one legal hold that satisfies the stricter of the two preservation standards on each point; do not run parallel notices that contradict each other.
- ☐ Host UK data in the UK; give US counsel access under a transfer mechanism, or transfer only the responsive set.
- ☐ Prepare two sets of privilege instructions (Section 13) and obtain a Rule 502(d) order.
- ☐ Agree a single production specification with day-month-year dates and one time zone.
- ☐ Remember CPR 31.22: documents disclosed in English proceedings cannot simply be reused in the US case without permission.
- ☐ Criminal channels are separate: the UK-US Data Access Agreement (in force 3 October 2022) covers serious crime only.

Data protection in disclosure

Every disclosure exercise is large scale processing of personal data, much of it belonging to people who have nothing to do with the dispute. Data protection law does not stop disclosure. It shapes how disclosure is done.

How the principles apply

REQUIREMENT	APPLICATION TO DISCLOSURE
Lawful basis (Art 6)	Usually legal obligation (Art 6(1)(c)), since disclosure is required by rules of court and court order, or legitimate interests (Art 6(1)(f)) for pre-action work and investigations. Consent is rarely appropriate.
Special category and criminal offence data (Arts 9 and 10)	The legal claims condition in Art 9(2)(f), and the equivalent condition in DPA 2018 Schedule 1 paragraph 33 for criminal offence data. Health, union membership and similar data turn up in almost every mailbox.
Data minimisation (Art 5(1)(c))	Scope by custodian and date, cull before review, restrict reviewer access, redact irrelevant personal data that is confidential, and produce only what the order requires.
Storage limitation (Art 5(1)(e))	Release holds and delete hosted data when the matter is over (Section 14).
Security (Arts 5(1)(f) and 32)	Encryption in transit and at rest, access controls, logging, vetted staff, tested incident response. Ask the provider for evidence, not assurances.
Processors (Art 28)	A written processing agreement with the eDisclosure provider and any sub-processor, including AI services. The law firm and client will usually each be controllers.
Impact assessment (Art 35)	Appropriate for large collections, mobile device extractions, special category data, novel technology and any cross-border transfer.
Transparency and the exemptions	DPA 2018 Schedule 2 paragraph 5 disapplies the listed provisions (including transparency and objection rights) to the extent that they would prevent disclosure required by an enactment, rule of law or court order, or necessary for legal proceedings, legal advice or establishing, exercising or defending legal rights. Paragraph 19 exempts privileged material from subject access.
International transfers (Ch V)	See Section 16.

What the Data (Use and Access) Act 2025 changed

The Act received Royal Assent on 19 June 2025, and the regulator's guidance now records that all of its data protection provisions are in force. It also replaces the Information Commissioner's Office with a new body, the Information Commission, from 30 September 2026; the initials ICO remain. For disclosure lawyers the main points are:

- **Subject access searches.** Section 78 confirms that a controller need carry out only a "reasonable and proportionate" search in response to a subject access request, with effect treated as running from 1 January 2024. This codifies earlier case law and guidance and gives a firmer footing for resisting requests designed to impose cost.
- **Stop the clock.** The time limit for responding can pause while the controller seeks clarification it reasonably needs.
- **Recognised legitimate interests.** A new lawful basis for listed public interest purposes, including crime prevention and safeguarding, without a balancing test. It will be relevant in some investigations.
- **International transfers.** A revised "data protection test" asks whether the standard of protection in the destination is not materially lower than in the UK.
- **Automated decision-making.** The reformed rules are relevant where AI tools are used in ways that significantly affect individuals. Classifying documents for review will not usually meet that threshold, but document the analysis.

Subject access requests as a litigation tool

Individuals increasingly serve subject access requests before or alongside a claim. The request cannot be refused merely because its purpose is to obtain documents for litigation (*Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74). The differences from disclosure matter:

	SUBJECT ACCESS REQUEST	DISCLOSURE
Entitlement	The requester's own personal data, not documents as such	Documents relevant to the issues
Timing	One month, extendable by two for complex requests	As ordered by the court
Search	Reasonable and proportionate	Reasonable, under CPR 31.7 or the Model ordered
Withholding	Exemptions for privilege, third party data, negotiations, management forecasting and others	Privilege; limited redaction
Use of material	Unrestricted	CPR 31.22 restriction
Enforcement	ICO complaint or court order under DPA 2018 section 167	Court, within the proceedings

Run a contentious subject access response as a small disclosure project: define the search, document it, review for exemptions, redact third party data, and keep the audit trail. What is released will be read by the opponent's litigation team, and inconsistencies with later disclosure will be noticed.

KEY POINTS

- Record the lawful basis and the minimisation steps; sign an Article 28 agreement with every provider.
- Schedule 2 paragraph 5 removes the obstacles to court ordered disclosure, not the duty to handle data carefully.
- Treat a contentious subject access request as the first round of disclosure.

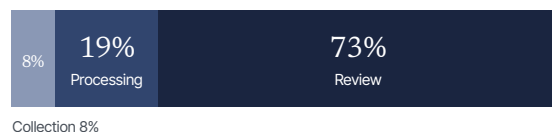
Costs and proportionality

Disclosure is usually the largest single cost in document-heavy litigation, and under English costs shifting the loser pays for it twice. Proportionality is the legal test; cost control is the practical skill.

Where the money goes

FIGURE 19 Where disclosure money goes, and the six levers that move it

SHARE OF DOCUMENT PRODUCTION COST (RAND, 2012)



What this means

A pound saved before review is worth more than a pound saved in review, because every document removed upstream is never hosted, read, quality-checked, redacted or produced.

SIX LEVERS THAT ACT BEFORE REVIEW



Custodians

Tier and justify by issue



Date range

Set issue by issue



Sources

Search where the evidence is



Culling and search

De-duplicate, thread, test terms



Review method

Active learning, validated AI



Staging

Phase it; stop when enough

Review dominates. The cost split is from the RAND Institute for Civil Justice study of US corporate litigants (2012); the proportions remain a fair guide, although technology has reduced the absolute cost of each stage. Every lever on the right acts before review begins.

The legal test

The overriding objective requires cases to be dealt with justly and at proportionate cost (CPR 1.1). Under PD57AD an order for Extended Disclosure must be reasonable and proportionate having regard to the overriding objective and the seven factors in paragraph 6.4. Arguments about scope are won with evidence on each factor, not adjectives.

PARAGRAPH 6.4 FACTOR	EVIDENCE TO BRING
(1) Nature and complexity of the issues	The List of Issues for Disclosure, tied to the pleadings.
(2) Importance of the case, including non-monetary relief	Value, reputational and regulatory consequences, wider significance.
(3) Likelihood of documents with probative value	Sampling results and key documents found in early assessment.
(4) Number of documents	Volumes by custodian and source; hit reports for each proposed term.
(5) Ease and expense of search and retrieval	Provider estimates; restoration costs for backups; mobile extraction costs.
(6) Financial position of each party	Relevant where one side seeks to impose disproportionate cost on the other.
(7) Expedition, fairness and proportionate cost	Timetable impact and a costed comparison of the competing proposals.

The DRD requires cost estimates for the disclosure proposed, and the disclosure phase of Precedent H must be consistent with them. A party whose budget assumed Model C and who then proposes Model D on every issue has a credibility problem. *Nichia Corp v Argos Ltd* [2007] EWCA Civ 741 remains the reminder that a perfect search is not required: the question is what is proportionate for this case.

The six levers

01 Custodians

Each Tier 1 custodian adds tens of thousands of documents. Tier rigorously and justify each name by issue.

02 Date range

Set by issue, not for the case as a whole. A six month reduction often removes a fifth of the volume.

03 Sources

Search the systems where the evidence is, not every system that exists. Park backups and marginal sources with reasons recorded.

04 Culling and search

De-duplication, threading, file type filters and tested search terms (Sections 09 and 10).

05 Review method

Continuous active learning or validated generative AI first pass can halve review volume (Section 12).

06 Staging

Disclose in phases: key custodians and issues first, then decide with the opponent or the court whether the next phase is justified by what the first one found.

Reading a provider's price

Pricing models vary: per gigabyte for processing and monthly hosting, per user licences, per document for review, fixed fees for defined phases, or all-in subscriptions. None is inherently better. Ask for a total cost of matter estimate based on your actual volumes and timetable, with assumptions stated, and check in particular how long hosting will last, whether data is charged at collected or processed size, what analytics and review technology cost extra, and what it costs to export and close the matter.

Illustrative first-pass review cost for 61,400 documents

APPROACH	DOCUMENTS READ	INDICATIVE COST
Linear review of everything	61,400	£52,000 to £86,000
Threading and near-duplicate suppression, then linear	about 43,000	£37,000 to £60,000
Continuous active learning, stopped on validation	about 26,000 plus 1,500 validation sample	£23,000 to £39,000

Assumes £0.85 to £1.40 per document all-in for first-level review. Illustrative only; actual figures depend on document type, complexity and team.

THE 2026 SURVEY ON COST

In the Disclosure Review Working Group's survey (summary published July 2026), 67% of respondents said disclosure costs had risen under PD57AD. Much of that cost is front-loaded negotiation over Issues for Disclosure and the DRD. The practical answer is to keep the list of issues short, propose Models that match what each issue really needs, and resolve disagreements with data (hit counts, samples, cost estimates) at a short guidance hearing.

Choosing technology and providers

The platform matters less than the people running it and the discipline around it. Choose for the matter in hand, test the claims and keep the ability to leave.

The landscape in brief

OPTION	STRENGTHS	WATCH FOR
Built-in tools of the client's own platform (for example Microsoft Purview, Google Vault)	Hold, search and export at source; no data movement; good for preservation and first scoping.	Limited review features; licence tier dependent; indexing limits; the client's IT team becomes part of the evidential chain.
Self-service cloud review platforms	Fast to start, simple pricing, adequate for small and medium matters.	Limited forensic capability; chat and mobile handling varies; check validation features and export rights.
Enterprise review platforms run by a specialist provider	Full processing control, advanced analytics and review technology, project management, defensible reporting, expert support.	More cost components; quality depends on the team assigned.
Forensic laboratory	Device imaging, mobile extraction, deleted data recovery, authenticity analysis, expert evidence.	Needed whenever the integrity or history of data is in issue; many review vendors subcontract it.

A selection scorecard

CRITERION	WHAT GOOD LOOKS LIKE
Security	ISO 27001 certification, Cyber Essentials Plus, recent independent penetration test, encryption at rest and in transit, role based access, full audit logging.
Data location	UK hosting by default; named sub-processors; no transfer outside the UK without instruction.
Forensic capability	In-house examiners, documented chain of custody, validated tools, ability to give expert evidence.
Processing quality	Transparent settings, exceptions reporting, time zone control, robust handling of chat, mobile and collaboration data.
Review technology	Continuous active learning and, if offered, generative AI with validation workflows, prompt logging and clear data use terms.
Reporting	Reports that map to the DRD and the Disclosure Certificate: volumes, searches, hit counts, validation results.
Portability and price	Standard export formats, a stated price for export and deletion, a total cost of matter estimate with caps or alerts, and a clear hosting end date.
People	A named project manager, realistic availability, experience in the relevant court and with the relevant data types.
Independence and compliance	Conflicts checked; ICO registration; Article 28 processing terms; professional indemnity and cyber insurance.

PROFESSIONAL DUTIES WHEN OUTSOURCING

Instructing a provider does not transfer responsibility. Solicitors remain accountable for the work and must supervise it effectively (SRA Code, paragraph 3.5), keep client affairs confidential (paragraph 6.3), and, as controllers, use only processors providing sufficient guarantees (UK GDPR Article 28(1)). Record the due diligence. The question bank for providers is in Section 25.

Beyond the High Court: other forums and jurisdictions

The data and the forensic disciplines are the same everywhere. The rules about who must hand over what are not.

FORUM	REGIME	WHAT IS DIFFERENT
County Court and High Court outside the Business and Property Courts	CPR Part 31 and PD31B	The CPR 31.5(7) menu applies in multi-track and intermediate track claims (personal injury claims excepted); PD31B applies on the multi-track. Fast track and intermediate track claims run within fixed costs, so proportionality is acute: targeted collection and agreed searches are essential.
Employment Tribunal	Employment Tribunal Procedure Rules 2024; case management orders	Disclosure is by order and usually by list with a joint bundle. Volumes are smaller but mobile messaging, HR systems and subject access requests dominate. No general costs shifting, so economy matters.
Competition Appeal Tribunal	CAT Rules 2015 and the Tribunal's practice directions	Tailored, staged disclosure under active case management, with confidentiality rings as standard. PD57AD does not apply: in <i>Coll v Alphabet Inc</i> [2024] CAT 25 an application for a known adverse documents order was refused.
Family (financial remedies)	Family Procedure Rules; Form E	A duty of full and frank financial disclosure. Self-help is unlawful: a spouse may not take the other's confidential documents (<i>Imerman v Tchenguiz</i> [2010] EWCA Civ 908). Forensic examination of devices needs consent or an order.
Arbitration seated in England	Arbitration Act 1996 as amended by the Arbitration Act 2025; institutional rules; usually the IBA Rules on the Taking of Evidence (2020)	No general disclosure. Parties produce what they rely on and make narrow, specific requests (Article 3), usually in a Redfern schedule. Article 9.2 lists grounds of objection including privilege, burden, confidentiality and proportionality. Section 44 of the 1996 Act, as amended, confirms that court orders in support of arbitration can be made against third parties.
Regulatory and criminal investigations of companies	Statutory powers, for example FSMA 2000 section 165, Criminal Justice Act 1987 section 2, Competition Act 1998 section 26	Compelled production on the regulator's timetable, with criminal offences for destruction or falsification. Privilege is protected; confidentiality generally is not. The workflow is the same; the margin for error is smaller.
Scotland	Commission and diligence for the recovery of documents (Court of Session Rules, Chapter 35; equivalent sheriff court rules)	No general duty of disclosure. A party applies for approval of a specification of documents, which is served on the holder (the "haver"). Calls must be specific and tied to the pleadings. Preservation and forensic method matter just as much.
Northern Ireland	Order 24, Rules of the Court of Judicature (NI) 1980	Still called discovery, by list of documents, with a relevance test closer to the pre-1999 English position. No PD57AD equivalent.

Criminal proceedings

Criminal disclosure runs on different principles. Under the Criminal Procedure and Investigations Act 1996 and its Code of Practice, investigators must pursue all reasonable lines of enquiry, whether they point towards or away from the suspect, and must record and retain relevant material. The prosecutor must disclose material that might reasonably be considered capable of undermining the prosecution case or assisting the accused. The Attorney General's Guidelines on Disclosure (2024 edition) contain detailed guidance on digital material, including proportionate examination of devices, the use of search tools and analytics, and engagement with the defence on parameters. The CPS Disclosure Manual deals with digital material in Chapter 30.

In July 2026 the Government published its response to the Independent Review of Disclosure and Fraud Offences, *Modernising the Criminal Disclosure Regime*. It commits to amending the statutory Code so that technology, including AI, can be used for scheduling and review of unused material, and to a protocol on AI use, and it undertakes to explore a pilot of an intensive disclosure regime for the heaviest cases. Expect the criminal and civil toolkits to converge further.

A defence checklist for digital material

- ☐ Ask early what devices and accounts were seized, what was extracted from each, with which tool, version and settings, and what was not examined.
- ☐ Ask what search terms, date ranges and analytical tools were applied to decide what was relevant, and whether the defence was consulted on the parameters as the Guidelines encourage.
- ☐ Obtain the extraction reports and, where authenticity or completeness is in doubt, access to the forensic image for an independent examiner.
- ☐ Use the defence statement and section 8 of the 1996 Act to request specific categories of digital material, with reasons tied to the issues.
- ☐ Check the schedules of unused material against what the extraction reports show exists.
- ☐ Forensic science activities carried out for the criminal justice system in England and Wales are subject to the Forensic Science Regulator's statutory Code of Practice (version 2 in force from 2 October 2025), which includes digital forensics. Ask whether the unit that did the work is compliant, and for which activities.



PART FIVE

The toolkit

Worked examples, the mistakes that recur, red flags, when to call a forensic expert, question banks, model wording, a master checklist, a glossary and the sources.

21	Worked examples	60
22	Common mistakes and technical limitations	62
23	Red flags	63
24	When to involve a digital forensic expert	64
25	Questions to ask: client, opponent, provider	65
26	Suggested wording	66
27	Master checklist	68
28	Glossary	69
29	References and further reading	71
30	How a specialist laboratory can assist	73

• SECTION 21 • TOOLKIT — THREE FICTITIOUS MATTERS

Worked examples

Three realistic matters showing the lifecycle in use. All parties, people and figures are fictitious.

EXAMPLE 1 • COMMERCIAL DISPUTE UNDER PD57AD

Aldgate Components Ltd v Harlow Precision Engineering Ltd

A supply agreement ends badly. Aldgate alleges late and defective deliveries and misuse of its confidential pricing; its former commercial director, James Marsh, has joined Harlow. The claim is issued in the Business and Property Courts.

WHEN	WHAT THE LEGAL TEAM DID	WHY IT MATTERED
Day 1	First meeting. Written preservation advice the same day. Asked where people really communicated: email, Teams, a bid team WhatsApp group.	PD57AD paragraph 4.4 duty discharged and recorded.
Days 2 to 12	Administrator exported Microsoft 365 audit logs (one year retention) and suspended a 12 month Teams retention policy. Hold notices to 30 people in three tiers.	The logs showed bulk deletions from Marsh's mailbox in February 2025. A week later they would have started to roll off.
Weeks 2 to 4	Marsh's returned laptop, quarantined by IT, was forensically imaged. His phone had been wiped and reissued on departure. Counterpart mailboxes and monthly backup snapshots identified as alternative paths.	The mailbox gap from November 2024 to March 2025 was largely rebuilt from recipients' copies and two snapshots.
Months 2 to 4	Targeted collection for nine Tier 1 custodians: 412 GB, 2.81 million items. De-duplication removed 44%. Early assessment found the key pricing thread and produced a costed review estimate.	The client saw its best and worst documents before pleading, and the DRD was drafted from real numbers.
DRD phase	Five Issues for Disclosure. Hit reports exchanged; one of the opponent's proposed terms dropped (34,000 unique hits at 2% precision) and one narrowed to 3,100 documents. Continuous active learning proposed with shared validation.	Two points only went to the court, decided at the case management conference in under an hour.
Order	Model D with technology assisted review on pricing and the CAD files; Model C on delivery, quantum and the counterclaim, including a request for access logs to two named CAD folders for a five month window in native CSV.	The Model C log request went to the heart of the data theft allegation at a fraction of the cost of a Model D search.
Review	61,400 documents in the review population. Review stopped after about 26,000 on a passed elusion test. Three adverse threads escalated and listed.	The Disclosure Certificate was signed with a complete record behind it.

Lesson. The decisive evidence (deletion logs, a quarantined laptop) was captured in the first fortnight. Everything later depended on that.

EXAMPLE 2 • TEAM MOVE AND DATA THEFT

Halden Recruitment Ltd and two departing directors

Two directors of a recruitment business resign on the same day and start a competitor. Clients begin to move within weeks. Halden suspects that the candidate database went with them.

1. **Preserve before confronting.** The solicitors advised that the directors' laptops, phones and accounts be secured before any letter was sent. IT had been about to reissue the laptops.
2. **Forensic imaging and targeted analysis.** A forensic examiner imaged both laptops and analysed user activity for the 60 days before resignation: USB device history, cloud storage clients, recently opened files, browser history and print jobs. One laptop showed a personal cloud storage client installed three weeks before resignation and 4,200 files synchronised to it; the other showed a bulk CRM export to CSV at 23:10 on the last working day and a USB drive connected minutes later.
3. **Corroborate from other sources.** CRM audit logs confirmed the export. Email gateway logs showed forwarding to a personal address. The source architecture approach produced three independent records of the same act.
4. **Interim relief.** With an expert report in support, Halden obtained an order for delivery up and for the independent imaging of the directors' personal devices and cloud accounts, with a search protocol protecting private material and privileged communications.
5. **Proportionate disclosure.** Disclosure was confined to the forensic findings, the logs and communications with 40 named clients over a four month window.

Lesson. This was a forensic case from the first hour. A conventional email review would have found little; the evidence was in system artefacts and logs that ordinary collection does not capture and that routine IT housekeeping would have destroyed.

EXAMPLE 3 • CROSS-BORDER

Northmere Analytics Ltd and a US document request

Northmere, the UK subsidiary of a Delaware company, holds the engineering records relevant to a patent and trade secrets action against its parent in the Northern District of California. US counsel asks for "everything from the UK team" within 30 days.

1. **Control and obligation.** US counsel advised that the parent would be treated as having control of the subsidiary's documents for Rule 34 purposes. Refusal was not an option; the question was how.
2. **One hold, two standards.** A single legal hold was issued to UK custodians meeting both the US reasonable anticipation standard and UK good practice.
3. **Minimise in the UK.** Data for eleven custodians was collected, processed and hosted in London. Agreed search terms and date ranges were applied and review was carried out in the UK platform, with US counsel given remote access to the responsive set only under an International Data Transfer Agreement.
4. **Transfer.** Only responsive documents were exported to the US, under the Article 49(1)(e) legal claims exception with a written necessity assessment, after redaction of irrelevant personal data (HR matters, health information, family messages) and with special category data flagged.
5. **US protections.** A protective order restricted use to the litigation and allowed attorneys' eyes only designation; a Rule 502(d) order protected against privilege waiver. Two privilege protocols were applied because several UK in-house communications that were privileged under US law would not have been under English law, and the reverse.

Lesson. The US court received what it needed on time, and the UK company could show its employees and, if asked, the Information Commissioner a documented, proportionate process.

Common mistakes and technical limitations

Fifteen mistakes that recur

#	MISTAKE	BETTER PRACTICE
1	Preservation advice given orally, late, or not at all	Written advice on day one; written client confirmation on file.
2	Asking people not to delete, without suspending system deletion	Central suspension first; notices second.
3	Forgetting chat, mobile and personal accounts	Ask where people really talk; put the answers in the DRD.
4	Letting leavers' accounts and devices be recycled	Disputes check in the leaver process; image before reissue.
5	Custodian or IT self-collection	Supervised, logged, forensically sound collection.
6	Untested keywords agreed in a hurry	Hit reports, samples, null set testing, then agreement.
7	Ignoring the exceptions report	Review it, resolve what matters, record the rest.
8	No agreed time zone	Fix one zone in the DRD and production protocol.
9	Starting review without a protocol	Written protocol, training, decision log, daily quality control.
10	Using review technology without telling the other side	Transparency through the DRD; agreed validation.
11	Inconsistent privilege calls across duplicates and threads	Consistency reports before every production.
12	Cosmetic redaction	Burned-in redaction, regenerated text, metadata scrubbed, checked.
13	Over-disclosure "to be safe"	Apply the issues; PD57AD paragraph 3.1(6).
14	Not interrogating the other side's production	Intake checks and a specific gaps letter.
15	No audit trail	Contemporaneous logs at every stage, kept with the file.

What the technology cannot do

LIMITATION	CONSEQUENCE
Deleted data is not always recoverable	Solid state drives, full disk encryption, mobile operating systems and cloud storage leave far less recoverable residue than older hard disks did. Speed of preservation matters more than ever.
End to end encryption	Providers of encrypted messaging cannot supply message content. The handset, a linked device, or a backup is the only source.
Locked and updated phones	Extraction capability depends on model, operating system version and lock state, and changes with each software release. Some devices cannot be fully extracted without the passcode.
Search is only as good as the text	Poor scans, handwriting, images and audio are invisible without OCR or transcription, both of which make errors.
Time stamps are easy to misread	Time zones, daylight saving, server and device clock differences and application quirks all affect recorded times. Sequence evidence should be interpreted by someone who knows the artefacts.
Metadata can be altered	File system dates change through ordinary copying and can be set deliberately. Authenticity opinions rest on multiple corroborating artefacts, not one field.
Machine learning and AI are probabilistic	They rank and classify with measurable error. Validation is the only way to know how much.
Linked files, versions and logs expire	The platform may hold only the current version of a linked document, and audit data that would prove who did what is kept for a limited period fixed by licence and configuration.

Red flags

Any one of these justifies stopping to ask questions. Several together usually mean the matter has become a forensic one.

In your own client's account

- "IT has already pulled the emails" or "we've sent you everything relevant".
- A key custodian has left and nobody knows what happened to the laptop, phone or mailbox.
- Business was done on WhatsApp, Signal or personal email and there is no policy covering it.
- Disappearing messages were on, or were turned on after the dispute began.
- A new phone, a factory reset or a "lost" device around the time of key events.
- Retention periods nobody can state, or an administrator who is also a witness.
- Reluctance to let anyone independent look at a device or account.

In the other side's disclosure

- Custodians with implausibly few documents, or months with none.
- Emails without attachments, replies without the original, threads that start in the middle.
- Key documents produced only as PDFs or screenshots, with natives "unavailable".
- Metadata fields blank, uniform or inconsistent with content (a letter "created" after it was sent).
- A helpful document that surfaces late, from an unexpected source.
- Channels listed in the DRD that do not appear in the production.
- A disclosure certificate signed by someone with no evident knowledge of the search.

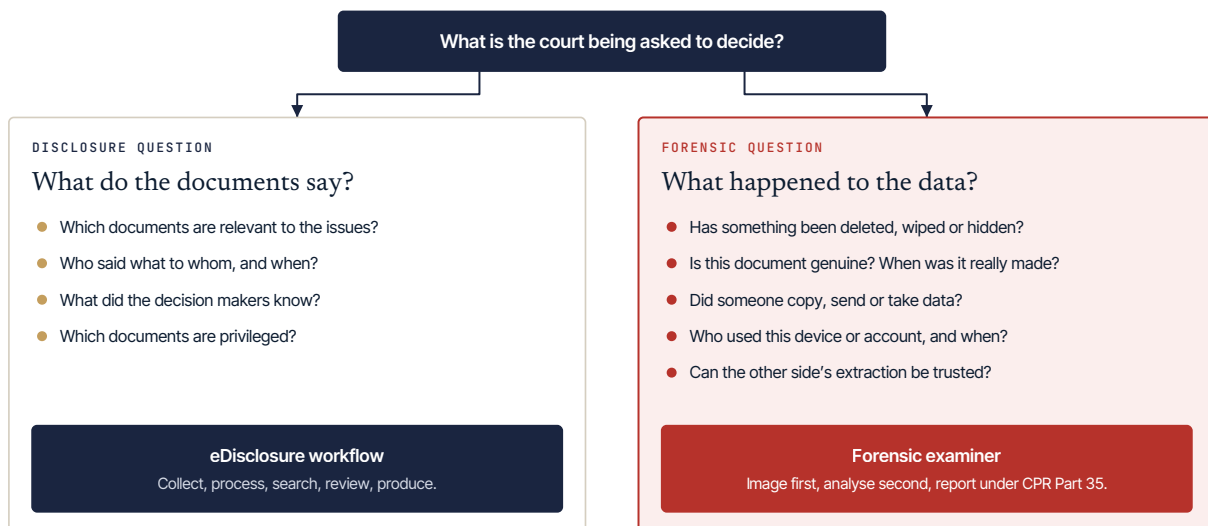
In the data itself

- Bulk deletions, mailbox rule changes or mass downloads in audit logs near key dates.
- USB storage, personal cloud sync or large email forwards shortly before a resignation.
- Wiping or "cleaner" utilities installed or run; system clock changes.
- Documents whose fonts, software version or metadata post-date their purported date.
- An exceptions report full of encrypted containers nobody can open.
- Validation results that fail, or that nobody can produce.

When to involve a digital forensic expert

eDisclosure asks what the documents say. Digital forensics asks what happened to the data: who created it, who touched it, what was deleted, and whether it is what it claims to be.

FIGURE 20 Disclosure question or forensic question?



If any answer on the right applies, take forensic advice before anything else is done to the device or account. The first hours determine what can later be proved.

TRIGGER	WHAT A FORENSIC EXAMINER ADDS
Suspected deletion or concealment	Recovery where possible; proof that deletion occurred, when and by which account; identification of wiping tools; reconstruction from alternative sources.
Disputed authenticity	Examination of native files, metadata, fonts, software versions, email headers and server records to test whether a document could have been created when and how it is claimed.
Departing employees, data theft and attribution	User activity timelines (external devices, cloud uploads, file access, printing, forwarding) and attribution from login records, device identifiers and network logs.
Mobile devices and messaging	Lawful, complete extraction; recovery of deleted messages where available; presentation of chats in evidential form.
Hostile custodians and imaging orders	Independent collection under a protocol both sides and the court can trust, including execution of delivery up and imaging orders with privacy and privilege safeguards.
Challenging the other side's digital evidence	Review of extraction reports and methodology in civil or criminal proceedings; identifying what was not examined.

How to instruct

- **Early and in writing.** State the questions, not the answers you hope for.
- **Preserve first.** Image before analysing, so the opponent's expert can repeat the work.
- **Separate roles.** Decide whether the examiner is an adviser (whose communications may be privileged) or a Part 35 expert (whose instructions may be disclosed), and plan any move from one role to the other.
- **Get permission.** Raise expert evidence at the case management conference with a defined issue and an estimate.
- **Know the limits.** Forensics can often show that an event occurred on a device and under which account. It can rarely prove alone who was at the keyboard or why.

Questions to ask: client, opponent, provider

Three question banks to lift into agendas, letters and tenders.

Questions for your client

1. Who was involved in the events, including assistants, leavers, contractors and advisers?
2. Which systems hold email, chat, documents and business records, and who administers each?
3. What are the actual retention settings for email, chat, file stores, backups and audit logs?
4. Has any automatic deletion been suspended? When, by whom, and is there a record?
5. Who has left since the events? What happened to their accounts, laptops and phones?
6. Did anyone use personal phones, personal email or messaging apps for this business? Which apps? Are disappearing messages on?
7. Are meetings recorded or transcribed? Are AI assistants in use, and is their history retained?
8. Which third parties hold relevant documents for you: IT providers, accountants, agents, former solicitors?
9. Which lawyers, internal and external, advised on these events? (For the privilege screen.)
10. Has anyone already searched for, collected, forwarded or deleted documents about this dispute?
11. Are there documents you already know are unhelpful? (The known adverse documents duty.)
12. Is any relevant data held outside the UK, or subject to another country's secrecy or data laws?
13. Is there a related regulatory enquiry, complaint, subject access request or insurance notification?
14. Who will sign the Disclosure Certificate, and do they understand what it confirms?
15. What is the budget, and who approves changes to it?

Questions for your opponent

1. When did your client first contemplate proceedings, and what preservation steps were taken, on what dates?
2. Which deletion processes were suspended, and which were not?
3. Which custodians and sources do you propose, and which have you excluded and why?
4. Have any custodians left? What became of their data and devices?
5. Do custodians use mobile messaging, personal email or collaboration platforms for work? How will these be collected?
6. What date ranges do you propose for each Issue for Disclosure?
7. What search terms do you propose, and will you share hit reports, including unique hits?
8. What review technology will you use, and how will it be validated? If none above 50,000 documents, why not?
9. How were documents collected, by whom, and with what tools?
10. What de-duplication, threading and time zone settings are applied?
11. In what format will you produce, with which metadata fields?
12. Are any relevant documents known to have been lost or destroyed? When and how?

Questions for a forensic or eDisclosure provider

1. Who will carry out collection? What are their qualifications and have they given evidence in court?
2. Which tools will be used for computers, mobile devices, Microsoft 365, Google Workspace and chat platforms, and how are they validated?
3. How will chain of custody and hash verification be documented? May we see a sample record?
4. Where will data be hosted, under which certifications, and who are the sub-processors?
5. Which processing settings are defaults, which will you ask us to decide, and how are exceptions reported and resolved?
6. How do you handle chat, short messages, linked files and version history?
7. Which review technologies are available, how are they validated, and what reports support the DRD and the Disclosure Certificate?
8. If generative AI is offered: which model, where does it run, is our data used for training, and how are prompts logged?
9. What is the total cost of matter on our volumes and timetable, and what do hosting, licences, analytics, productions and export each cost?
10. What happens to the data at the end, and what does certified deletion cost?
11. Can you host in the UK only, with remote access for overseas counsel?
12. Have you checked conflicts, and will you sign our processing agreement?
13. If methodology is challenged, who will give evidence about it?

Suggested wording

Starting points to adapt. Square brackets mark what must change. Keep each document short enough that the recipient will read it.

A • PRESERVATION ADVICE TO THE CLIENT (DAY ONE)

We have been instructed in relation to [the dispute with X concerning Y]. From now on [the Company] must preserve all documents that may be relevant to this dispute. “Documents” includes emails, chat and text messages (including on personal phones and apps such as WhatsApp), files, databases, recordings, backups and audit logs, in any location.

Please do the following within [48 hours] and confirm to us in writing when done: (1) suspend automatic deletion and retention policies affecting the people and systems listed in the schedule; (2) send the attached notice to the individuals listed, including former employees; (3) write to the third parties listed asking them to preserve documents they hold for you; (4) stop the reissue or wiping of any device used by those individuals; (5) tell us about any relevant deletion that has already happened.

Please do not search for, collect, forward or organise documents yourselves at this stage. We will arrange collection in a way that protects their evidential value. Failure to preserve documents can lead to serious consequences, including adverse inferences, costs sanctions and, in some circumstances, contempt of court.

B • LEGAL HOLD NOTICE TO EMPLOYEES AND FORMER EMPLOYEES

[The Company] is involved in a dispute with [X] about [one sentence, neutral description]. You have been identified as someone who may hold relevant documents.

With immediate effect, please do not delete, alter or discard any document relating to [topics], dated from [date] to the present, wherever it is held: work email and files, Teams or Slack messages, your phone (including WhatsApp, iMessage, Signal and text messages, whether the phone is personal or provided by the Company), personal email, home computers, notebooks and paper files. If disappearing messages are switched on for any relevant chat, please switch them off now and tell [name].

Please do not forward or copy documents to collect them; we will arrange that. If you are about to change your phone or computer, or to leave the Company, tell [name] first. This notice remains in force until you are told in writing that it has ended. Please reply to confirm that you have read and will follow it. Questions should go to [name, contact]. Please do not discuss the dispute by email or message with colleagues.

C • PRESERVATION LETTER TO THE OPPONENT

Our client anticipates proceedings against your client arising from [short description]. Your client is therefore under a duty to preserve documents that may be relevant (Practice Direction 57AD, paragraphs 3 and 4 [or: Practice Direction 31B, paragraph 7]).

We ask that your client immediately preserve, and suspend any automatic deletion of, documents held by or for [named individuals] for the period [dates], including in particular: (a) email and calendar data; (b) messages on [Teams / Slack / WhatsApp and similar applications], including on personal devices; (c) files in [systems]; (d) audit and access logs for [systems]; (e) backups covering that period; and (f) the computers and mobile devices used by [names], which should not be reset, reissued or disposed of.

Please confirm by [date] that these steps have been taken and the date on which each was taken. If any such material has already been lost, please say what, when and how. We reserve the right to refer to this letter on any question of costs or adverse inference.

D • INSTRUCTION TO A FORENSIC OR EDISCLOSURE PROVIDER

We act for [client] in [matter]. Please (1) carry out a forensically sound collection of the sources listed in Schedule 1, preserving all metadata, recording hash values at acquisition and maintaining a chain of custody record for each item; (2) retain the original images unaltered and work only on verified copies; (3) process the data using the settings in Schedule 2 (de-duplication: global at family level with all-custodian field; time zone: [UTC/UK]; date range: [dates]) and provide a processing report and exceptions report; (4) host the data in the United Kingdom with access limited to the users in Schedule 3; (5) not transfer any data outside the United Kingdom without our written instruction.

You act as our client's processor under the attached data processing terms. Please keep a contemporaneous log of all steps taken, sufficient for an independent examiner to repeat them, and be prepared to provide a witness statement describing your methodology. Please do not carry out any analysis of device contents beyond that described here without further instruction. [If expert evidence is contemplated: a separate letter of instruction under CPR Part 35 will follow.]

E • DRD WORDING FOR TECHNOLOGY ASSISTED REVIEW

The [Claimant] proposes to review the documents responsive to the agreed date ranges, custodians and search terms for Issues [2 and 3] using continuous active learning in [platform]. Review will continue until (a) the rate of relevant documents in consecutive batches falls below [x]% and (b) an elusion test on a simple random sample of [1,500] unreviewed documents, reviewed by a qualified lawyer, indicates that estimated recall is at least [75]%. The [Claimant] will provide the [Defendant] with the validation methodology and results (but not privileged documents or reviewer work product) within [7] days of completing validation and will notify the [Defendant] promptly if validation is not passed, with proposals for further steps.

Master checklist

A stage by stage list to copy into the matter file. If a box cannot be ticked, record why.

Govern and identify

- ☐ Regime identified (PD57AD, Part 31, other)
- ☐ Issues, custodians, sources and dates listed
- ☐ Custodians tiered; Tier 1 interviewed
- ☐ Source map includes chat, mobile, logs, third parties
- ☐ Control questions considered (group, agents, personal devices)

Preserve

- ☐ Written preservation advice sent on day one
- ☐ System deletion suspended; record kept
- ☐ Hold notices sent; acknowledgements logged
- ☐ Leavers' accounts and devices secured
- ☐ Third parties written to
- ☐ Logs exported; backup set isolated
- ☐ Client's written confirmation received
- ☐ Preservation letter to opponent considered

Collect

- ☐ Method chosen by reference to the issues
- ☐ No unsupervised self-collection
- ☐ Hashes and chain of custody recorded
- ☐ Mobile protocol agreed with custodians
- ☐ Processor agreement and impact assessment in place

Process and assess

- ☐ De-duplication, time zone and date settings approved
- ☐ Exceptions report reviewed
- ☐ Gaps and anomalies investigated
- ☐ Search terms tested; hit reports kept

- ☐ Cost estimate prepared; Precedent H aligned

- ☐ DRD section 2 completed from real data

Review

- ☐ Written protocol; team trained
- ☐ Privilege screen and privilege team in place
- ☐ Review technology agreed or disclosed; validation plan set
- ☐ Daily quality control; overturn rates tracked
- ☐ Known adverse documents list maintained

Produce

- ☐ Production protocol agreed
- ☐ Consistency and privilege checks run
- ☐ Redactions verified
- ☐ List, certificate and covering letter prepared
- ☐ Secure transmission; receipt logged

After exchange

- ☐ Opponent's production loaded and tested
- ☐ Gaps letter sent
- ☐ Authenticity notices considered (CPR 32.19)
- ☐ Expert evidence considered
- ☐ Continuing duty diarised

Close

- ☐ Hold released in writing
- ☐ Opponent's documents returned or destroyed
- ☐ Hosted data deleted; certificate obtained
- ☐ Audit trail archived with the file

Glossary

Adverse document

A document that contradicts or materially damages the disclosing party's case or supports the opponent's. Under PD57AD, "known" adverse documents must be disclosed whatever Model is ordered.

Audit log

A system record of user and administrator actions (sign-ins, file access, deletions, sharing). Retained for limited periods.

Bates number / document ID

A unique identifier stamped on or assigned to each produced document or page.

Chain of custody

The documented history of who held an item of evidence, when and what was done to it.

Clawback

An agreement or order for the return of privileged documents disclosed by mistake.

Clustering

Software grouping of documents by similar content without human-defined terms.

Confidentiality ring (club)

An order limiting inspection of sensitive documents to named individuals on the receiving side.

Continuous active learning (CAL)

Review technology that learns from every coding decision and continually re-ranks unreviewed documents.

Control

Physical possession, a right to possession, or a right to inspect or copy a document (CPR 31.8).

Custodian

A person or shared resource whose data may contain relevant documents.

Data map

An inventory of an organisation's information systems, their content, retention and export capability.

De-duplication

Removal of exact copies, identified by hash value, within a custodian or across the whole set (global).

De-NISTing

Removing known operating system and program files by comparison with the US National Institute of Standards and Technology reference list.

Disclosure Certificate

The signed confirmation under PD57AD that a party has understood and complied with its disclosure duties.

Disclosure Guidance

A short application under PD57AD paragraph 11, decided on the documents or at a hearing of up to 60 minutes, often called a Disclosure Guidance Hearing.

DRD

Disclosure Review Document: the court form recording Issues for Disclosure, proposed Models and the technical approach.

Early case assessment (ECA)

Using the processed data early to evaluate the merits, risks and cost of the dispute. Early data assessment measures the data itself.

EDQ

Electronic Documents Questionnaire under PD31B.

EDRM

The Electronic Discovery Reference Model, an industry framework for the stages of eDiscovery. Version 2.0 was released in September 2026.

Elusion rate

The proportion of relevant documents in the set that will not be reviewed, estimated from a random sample.

Ephemeral messaging

Messaging that deletes itself after a set time (disappearing messages).

ESI

Electronically stored information (the US term).

Exceptions report

The list of files that could not be fully processed (encrypted, corrupt, unsupported).

Extended Disclosure

Disclosure beyond Initial Disclosure under PD57AD, ordered issue by issue using Models A to E.

Family

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

Forensic image

A verified, bit for bit copy of a storage device, including deleted and unallocated areas.

Hash value

A digital fingerprint (for example SHA-256) calculated from content; any change produces a different value.

Initial Disclosure

Key documents provided with statements of case under PD57AD paragraph 5.

Issues for Disclosure

The key issues in dispute that the parties consider will need to be determined by reference to contemporaneous documents (PD57AD paragraph 7).

Legal hold

The process of suspending deletion and notifying custodians to preserve documents for a dispute.

Load file

A data file that tells a review platform how to import a production: document boundaries, metadata, text and images.

Metadata

Data about a document: system metadata (dates, paths), application metadata (author, revisions) and email headers.

Native format

The format in which a document was created and is ordinarily used (for example .msg, .xlsx).

Near-duplicate

Documents with highly similar text, such as successive drafts.

Norwich Pharmacal order

An order requiring a person mixed up in wrongdoing to disclose information, typically the wrongdoer's identity.

Null set

The documents not returned by a search or not selected by review technology.

OCR

Optical character recognition: converting images of text into searchable text.

Precision

Of the documents identified as relevant, the proportion that really are.

Predictive coding

First generation technology assisted review trained on a seed set.

Privilege log

A US-style list of withheld documents with the basis for each. English lists may describe by class.

Processing

Extraction of text and metadata, de-duplication and indexing to make data searchable.

Recall

Of all the relevant documents in the set, the proportion that were found.

Redfern schedule

The tabular form of document requests, objections and rulings used in arbitration.

Richness (prevalence)

The proportion of relevant documents in a population.

Section 1782

The US statute allowing discovery in aid of foreign proceedings.

Spoliation

The US term for destruction or alteration of evidence.

TAR

Technology assisted review: using machine learning to prioritise or classify documents for review.

Threading

Grouping emails into conversations and identifying the messages that contain all earlier content.

Unallocated space

Areas of a storage device not assigned to current files, where remnants of deleted data may survive.

Write blocker

Hardware or software that prevents any change to a source device during imaging.

References and further reading

Rules, practice directions and court guidance

- CPR Part 31, Disclosure and inspection of documents: [justice.gov.uk/courts/procedure-rules/civil/rules/part31](https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31)
- Practice Direction 31B, Disclosure of electronic documents: [justice.gov.uk/.../part31/pd_part31b](https://www.justice.gov.uk/.../part31/pd_part31b)
- Practice Direction 57AD, Disclosure in the Business and Property Courts: [justice.gov.uk/.../practice-direction-57ad-disclosure-in-the-business-and-property-courts](https://www.justice.gov.uk/.../practice-direction-57ad-disclosure-in-the-business-and-property-courts)
- Disclosure Review Document: [justice.gov.uk/_data/assets/pdf_file/0009/177471/disclosure-review-document.pdf](https://www.justice.gov.uk/_data/assets/pdf_file/0009/177471/disclosure-review-document.pdf)
- CPR Part 34 (witness summonses, evidence for foreign courts): [justice.gov.uk/.../part34](https://www.justice.gov.uk/.../part34); CPR Part 35 (experts): [justice.gov.uk/.../part35](https://www.justice.gov.uk/.../part35); CPR Part 46: [justice.gov.uk/.../part-46-costs-special-cases](https://www.justice.gov.uk/.../part-46-costs-special-cases)
- 193rd Practice Direction Update (CPR 31.12A, PD57AD paragraph 18.5): [justice.gov.uk/documents/193rd-pd-update.pdf](https://www.justice.gov.uk/documents/193rd-pd-update.pdf)
- Disclosure Review Working Group, survey update (July 2026): [judiciary.uk/update-disclosure-review-working-group-survey-of-legal-sector-stakeholders](https://www.judiciary.uk/update-disclosure-review-working-group-survey-of-legal-sector-stakeholders)
- General Guidance on Electronic Court Bundles: [judiciary.uk/guidance-and-resources/general-guidance-on-electronic-court-bundles](https://www.judiciary.uk/guidance-and-resources/general-guidance-on-electronic-court-bundles)
- Artificial Intelligence: Guidance for Judicial Office Holders (31 October 2025): [judiciary.uk/.../artificial-intelligence-ai-judicial-guidance-october-2025](https://www.judiciary.uk/.../artificial-intelligence-ai-judicial-guidance-october-2025)
- Civil Justice Council, Use of AI in preparing court documents: [judiciary.uk/.../cjc/current-work/use-of-ai-in-preparing-court-documents](https://www.judiciary.uk/.../cjc/current-work/use-of-ai-in-preparing-court-documents)

Legislation and regulatory guidance

- Data Protection Act 2018, Schedule 2: [legislation.gov.uk/ukpga/2018/12/schedule/2](https://www.legislation.gov.uk/ukpga/2018/12/schedule/2)
- Data (Use and Access) Act 2025: [legislation.gov.uk/ukpga/2025/18/contents](https://www.legislation.gov.uk/ukpga/2025/18/contents); ICO overview: ico.org.uk/.../data-use-and-access-act-2025
- ICO guidance on international transfers: ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers
- Evidence (Proceedings in Other Jurisdictions) Act 1975: [legislation.gov.uk/ukpga/1975/34](https://www.legislation.gov.uk/ukpga/1975/34); Protection of Trading Interests Act 1980: [legislation.gov.uk/ukpga/1980/11](https://www.legislation.gov.uk/ukpga/1980/11)
- Arbitration Act 2025: [legislation.gov.uk/ukpga/2025/4](https://www.legislation.gov.uk/ukpga/2025/4)
- Criminal Procedure and Investigations Act 1996: [legislation.gov.uk/ukpga/1996/25/contents](https://www.legislation.gov.uk/ukpga/1996/25/contents)
- Attorney General's Guidelines on Disclosure (2024): [gov.uk/government/publications/attorney-generals-guidelines-on-disclosure](https://www.gov.uk/government/publications/attorney-generals-guidelines-on-disclosure)
- CPS Disclosure Manual: [cps.gov.uk/legal-guidance/disclosure-manual](https://www.cps.gov.uk/legal-guidance/disclosure-manual)
- Forensic Science Regulator, statutory Code of Practice, version 2: [gov.uk/government/publications/forensic-science-activities-statutory-code-of-practice-version-2](https://www.gov.uk/government/publications/forensic-science-activities-statutory-code-of-practice-version-2)
- SRA Code of Conduct for Solicitors, RELs, RFLs and RSLs: [sra.org.uk/solicitors/standards-regulations/code-conduct-solicitors](https://www.sra.org.uk/solicitors/standards-regulations/code-conduct-solicitors)
- Law Society, Generative AI in legal disclosure (on the ILTA best practice guide): [lawsociety.org.uk/topics/civil-litigation/generative-ai-in-legal-disclosure-guide](https://www.lawsociety.org.uk/topics/civil-litigation/generative-ai-in-legal-disclosure-guide)

Cases (Find Case Law, The National Archives, unless stated)

- *Pyrrho Investments v MWB Property* [2016] EWHC 256 (Ch): caselaw.nationalarchives.gov.uk/ewhc/ch/2016/256
- *Triumph Controls v Primus* [2018] EWHC 176 (TCC): caselaw.nationalarchives.gov.uk/ewhc/tcc/2018/176
- *Earles v Barclays Bank* [2009] EWHC 2500 (Mercantile): caselaw.nationalarchives.gov.uk/ewhc/mercantile/2009/2500
- *Cabo Concepts v MGA Entertainment* [2022] EWHC 2024 (Pat): caselaw.nationalarchives.gov.uk/ewhc/pat/2022/2024
- *McParland & Partners v Whitehead* [2020] EWHC 298 (Ch): caselaw.nationalarchives.gov.uk/ewhc/ch/2020/298
- *Phones 4U v EE* [2021] EWCA Civ 116: caselaw.nationalarchives.gov.uk/ewca/civ/2021/116
- *Nichia v Argos* [2007] EWCA Civ 741: caselaw.nationalarchives.gov.uk/ewca/civ/2007/741
- *Douglas v Hello!* [2003] EWHC 55 (Ch): caselaw.nationalarchives.gov.uk/ewhc/ch/2003/55
- *Atlantisrealm v Intelligent Land Investments* [2017] EWCA Civ 1029: caselaw.nationalarchives.gov.uk/ewca/civ/2017/1029
- *R (Jet2.com) v CAA* [2020] EWCA Civ 35: caselaw.nationalarchives.gov.uk/ewca/civ/2020/35
- *Voltaire Capital Holdings v Watson* [2025] EWHC 1948 (Comm): caselaw.nationalarchives.gov.uk/ewhc/comm/2025/1948
- *R (Ayinde) v London Borough of Haringey* [2025] EWHC 1383 (Admin): [judiciary.uk](https://www.judiciary.uk) (PDF)
- *Coll v Alphabet Inc* [2024] CAT 25: catribunal.org.uk/judgments/14087721

United States and international

- Federal Rules of Civil Procedure (Rules 16, 26, 34, 37, 45): law.cornell.edu/rules/frcp; Federal Rule of Evidence 502: law.cornell.edu/rules/fre/rule_502
- Pending US rules amendments: uscourts.gov/forms-rules/pending-rules-and-forms-amendments
- 28 U.S.C. section 1782: law.cornell.edu/uscode/text/28/1782
- Hague Evidence Convention, status table and UK declarations: hcch.net/en/instruments/conventions/status-table/?cid=82
- The Sedona Principles, Third Edition: thesedonaconference.org/publication/The_Sedona_Principles; Commentary on Legal Holds, Second Edition: thesedonaconference.org/publication/Commentary_on_Legal_Holds
- EDRM model (EDRM 2.0, September 2026; CC BY 4.0, edrm.net): edrm.net/edrm-model/current
- IBA Rules on the Taking of Evidence in International Arbitration (2020): ibanet.org (PDF)
- ISO/IEC 27050-1:2019 Electronic discovery: iso.org/standard/78647.html; ISO/IEC 27037:2012 Digital evidence: iso.org/standard/44381.html
- Pace and Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery* (RAND, 2012): rand.org/pubs/monographs/MG1208.html

Reported cases not available on Find Case Law are cited by neutral or law report citation in the text. Rules and guidance change: check the current version before relying on any paragraph number.

How a specialist laboratory can assist

Most of what this guide describes can be run by a well organised legal team with a competent provider. A laboratory that combines electronic disclosure with digital forensics earns its place at the points where the two disciplines meet.

01 • FIRST FORTNIGHT

Preserve and collect

Preservation advice for IT teams, forensic imaging, mobile extraction, Microsoft 365 and Google Workspace collections, audit log capture, chain of custody.

02 • SCOPE AND COST

Process and assess

Processing with transparent settings, early case assessment, tested search terms, hit reports and cost estimates for the DRD and Precedent H.

03 • REVIEW AND PRODUCE

Host and deliver

UK hosted review, continuous active learning with validation, privilege and redaction workflows, court-ready productions and bundles.

04 • WHEN IT IS CONTESTED

Investigate and testify

Deleted data, authenticity, data theft and user activity analysis; independent examiner roles under court orders; CPR Part 35 and criminal expert evidence.

Computer Forensics Lab has provided digital forensic and electronic disclosure services from London since 2007, working for claimants and defendants, prosecution and defence, and for US counsel who need evidence collected in the United Kingdom to a standard that will survive cross-examination on either side of the Atlantic. Examiners respond to new enquiries the same working day, and every initial scoping conversation is confidential.

DISCLAIMER

This publication provides general information about electronic disclosure, eDiscovery and digital forensics as at September 2026. It is not legal advice and should not be relied on as such. The law, court rules, practice directions and technology described change frequently, and their application depends on the facts of each matter. Readers should take advice from a suitably qualified lawyer in the relevant jurisdiction before acting. References to United States law are a summary for comparison only. Worked examples, names, figures, dashboards and records are fictitious and illustrative. Product and platform names are the property of their respective owners and are mentioned for identification only; no endorsement is implied. © 2026 Computer Forensics Lab Ltd. All rights reserved.



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.



SCAN TO CONTACT
e-discovery.uk
+44 (0)20 7164 6971

NEW ENQUIRIES

+44 (0)20 7164 6971

EMAIL

info@e-discovery.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