



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

London digital forensics & e-discovery · Established 2007

Known Adverse Documents in the Digital Age

Methodology, People and the Places Nobody Searches

The duty to disclose known adverse documents is the moral core of modern disclosure, and the digital age has made it harder to perform honestly: knowledge is fragmented across people, damaging material concentrates in informal channels, and the repositories where bad news lives are rarely the ones anyone searches. This guide explains the duty, and the three pillars of identifying adverse electronic documents in practice: search methodology designed to find the case against you, a structured census of employee knowledge, and a deliberate sweep of the unusual repositories.

⌚ Estimated reading time: 29 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its eDiscovery arm, **e-discovery.uk**, builds the machinery this duty depends on: neutral, issue-driven search design that finds bad news as readily as good, review workflows with adverse-document coding and escalation built in, and the audit trail that shows the duty was performed rather than avoided. The laboratory side recovers what the duty sometimes requires finding: deleted threads, cleared chats and the documents whose absence is itself the problem, reported under CPR Part 35 and CrimPR Part 19 where needed.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

ISO 27001-ALIGNED SECURITY

ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES

PD 57AD / DRD EXPERIENCE

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: a human duty in a machine estate
- 03 The legal anatomy of the duty
- 04 Why the digital age changes everything
- 05 Pillar 1 · Search methodology matters
- 06 Pillar 2 · Employee knowledge matters
- 07 Pillar 3 · Unusual repositories matter
- 08 The identification programme, step by step
- 09 Handling an adverse find
- 10 Worked examples
- 11 Common mistakes and technical limitations
- 12 Questions to ask · Suggested wording
- 13 Checklist and red flags · When to involve a digital forensic expert
- 14 Frequently asked questions
- 15 Glossary · References · Disclaimer · How a specialist laboratory can assist

Executive summary

THE HEADLINE POINT: THE DUTY, AND THE THREE PILLARS OF PERFORMING IT

Under PD 57AD, a party must disclose documents it knows to be adverse (documents that contradict or materially damage its own case, or support its opponent's, on the issues in dispute) regardless of which disclosure Model applies, regardless of whether any search would have found them, and continuing until proceedings end. "Known" is a human test: for a company, awareness runs through the people with accountability or responsibility for the events in dispute or for the conduct of the proceedings, including those who have since left. The digital age makes honest performance genuinely hard: damaging material is more likely to exist, it concentrates in informal channels, and the knowledge of it is scattered across people and systems. Organisations that perform the duty well run three disciplines together: **search methodology** designed neutrally enough to find the case against them, not just the case for them; a structured census of **employee knowledge**, asking the adverse question directly of the people whose awareness counts, leavers included; and a deliberate sweep of the **unusual repositories** (chat, drafts, incident logs, private notes, the investigation file) where bad news actually lives.

- **The duty is personal, continuing and certificate-backed.** It attaches whatever Models are ordered (including none), it survives every milestone until judgment or settlement, and the disclosure certificate confirms compliance with it, signed by a human.
- **Wilful blindness is the modern risk.** A party cannot search only for helpful material, decline to ask its people the awkward question, leave the incident log unexamined, and then claim ignorance: the pattern itself invites inference, and courts and opponents have grown fluent at spotting it.
- **Reviews create knowledge.** Once a document surfaces in review, assessment sampling or witness preparation, it is known; the protective machinery is an escalation route every reviewer understands and a log that shows adverse finds moving promptly to the lawyers.
- **Handled early, adverse documents are manageable.** Assessed, privilege-checked, disclosed on the timetable and contextualised, they are almost always less damaging than their concealment, which converts a bad document into a conduct case.
- **The criminal analogue runs deeper.** Investigators' duties around material that undermines the prosecution or assists the defence (CPIA 1996 and the Attorney General's Guidelines) apply the same logic with sharper sanctions, and the disciplines in this guide transfer directly.

The problem in plain English: a human duty in a machine estate

The duty is drafted around a simple picture: a person knows about a damaging letter, so the letter is disclosed. The modern estate breaks that picture three ways:

- **Knowledge is fragmented.** The engineer knows the product failed in April; the operations manager holds the WhatsApp thread about it; the quality system holds the incident record; nobody in the legal chain knows all three exist, and no single mind connects the fact, the file and the case. "The company knew" is true; no individual performed the knowing in a way that reached the lawyers.
- **Bad news is informal.** Formal channels are drafted with an eye to the file; candour lives in chat, voice notes, drafts never sent, and the message that says what the board minute does not. The repositories most likely to hold adverse material are precisely the ones default searches skip.
- **Searches are built by advocates.** Terms drawn from your own case theory find your case; the case against you uses different words (the complaint's vocabulary, the internal nickname for the problem, the engineer's shorthand). A methodology that would genuinely surface adverse material has to be designed for it, on purpose.

So performance of the duty cannot be passive ("nothing came to our attention") and cannot be purely technological ("the agreed terms did not hit it"). It is an organised inquiry: ask the right people, search neutrally, look in the honest places, and record all three so the certificate's confirmation is a summary of work done. The three pillars that follow are that inquiry.

The legal anatomy of the duty

- **Adverse:** a document contradicts or materially damages the disclosing party's contended version of events, or supports the contentions of another party, on the issues in dispute. Materiality does the filtering: routine unhelpfulness is not the test, damage to the case on the issues is.
- **Known:** actual awareness, not constructive knowledge. For a company, awareness is assessed through persons with accountability or responsibility for the events giving rise to the proceedings or for the conduct of the litigation, and it expressly reaches such persons who have left: their former awareness counts, and reasonable steps to ask them are part of performance.
- **Search-independent:** the duty applies however limited the ordered disclosure (Model A included) and however reasonable the search that missed the document. It is the floor beneath every Model, which is exactly why light Models are tolerable to opponents and courts.
- **Timing:** known adverse documents are disclosed with Extended Disclosure where it is ordered on the relevant issue, and otherwise within the timetable the Practice Direction sets after the question of Extended Disclosure is resolved; a document becoming known later is disclosed promptly then. Initial Disclosure is not the vehicle: its limbs are documents relied on and documents necessary to understand the case.
- **Certification and sanction:** the Disclosure Certificate confirms the duty has been discharged; breach engages the court's full toolkit (adverse inference, costs, revocation and re-ordering, strike-out in extremity, and professional consequences for lawyers complicit in suppression). The duty ends only when the proceedings do.
- **Adjacent regimes:** outside the B&PCs, CPR 31.6 standard disclosure has always required disclosure of documents that adversely affect a party's own case, discovered through the reasonable search; the PD 57AD innovation is the knowledge-based duty that operates without one. In criminal proceedings, the CPIA 1996 disclosure test (material undermining the prosecution case or assisting the defence) and the Attorney General's Guidelines impose the same moral structure on investigators, with a Disclosure Management Document describing the methodology.

§ 0 4 · THE SHIFT

Why the digital age changes everything

DIGITAL REALITY	CONSEQUENCE FOR THE DUTY
Volume: everything is written down somewhere	The probability that adverse material exists approaches certainty in any real dispute; "there is nothing" is a claim about the inquiry, not the estate
Fragmented knowledge across people and systems	Performance requires assembling awareness deliberately: the census (§6), because no individual holds the whole picture
Candour migrates to informal channels	Chat, drafts, voice notes and personal devices are where adverse material concentrates: the repositories sweep (§7)
Reviews, assessments and witness prep surface documents daily	Knowledge is manufactured continuously through the litigation itself; escalation routes and logs (§8) turn that from a trap into compliance
Departed employees	They take awareness and leave documents; the duty reaches their former knowledge, so leaver interviews and preserved leaver data both matter
Deletion is easy and traceable	An adverse document deleted after contemplation converts a bad document into spoliation plus the bad document, usually recoverable by the other side's expert

Search methodology matters

A search designed to prove your case will not find the case against you. The methodological corrections:

- **Build terms from the issues, neutrally, in both vocabularies.** Alongside your case theory's language, include the complaint's vocabulary, the counterparty's terminology, and the internal shorthand for the problem (the nickname, the codeword, the recurring misspelling), which custodian interviews and core-document sampling surface. A term set that could only ever return supportive material is itself a red flag an opponent can argue from.
- **Code for adversity, expressly.** The review protocol includes an adverse or "hot against us" designation with a mandatory same-day escalation route to supervising counsel; reviewers are trained that flagging bad news is the job done well, not a problem caused. Without the code, adverse documents are seen, unlabelled and effectively lost inside "relevant".
- **Train TAR on relevance, not helpfulness.** Continuous active learning ranks by whatever the trainers reward; seed and training decisions must treat damaging-but-relevant documents as exactly as relevant as supportive ones, and QC sampling should check the model has not quietly learned advocacy.
- **Let sampling do its honest work.** Null-set and QC samples exist to measure what the method missed; when they surface adverse material, that is the system functioning, and the finds route to the escalation log like any others.
- **Document the neutrality.** The search protocol and methodology memo record that terms, coding and training were designed to find adverse material: the paper that answers any later suggestion of wilful blindness, and the cheapest insurance in this guide.

Employee knowledge matters

The duty's trigger is awareness in the right heads, so performance starts with a census of the heads:

- **Identify whose knowledge counts:** the people with accountability or responsibility for the events in dispute (decision-makers, doers, approvers) and for the litigation's conduct, mapped from the issue-source matrix and custodian work of the companion guides, and expressly including predecessors and leavers.
- **Ask the adverse question directly, and safely.** Each census interview includes, in terms: "Are you aware of any document (email, chat, note, recording, file, anywhere) that cuts against our position on these issues, or that the other side would want?" Framed as a safety question, with the explanation that early candour protects everyone and that the alternative is discovery by the opponent, it produces answers that the general "tell us about the project" interview never does.
- **Reach the leavers.** Reasonable steps to contact relevant former employees (the same people the preservation notices reached) with the same question, recorded whether they engage or not; their preserved accounts and devices are then the check on what memory offers.
- **Keep it neutral, and privileged.** Interviews are conducted under legal supervision, ask for awareness rather than argue the case, avoid anything resembling coaching, and are documented in privileged notes with the factual answers severable; sensitivities (whistleblowers, HR contexts, individuals with personal exposure) are handled with separate advice where needed.
- **Refresh on triggers.** Amended pleadings, exchanged witness statements, new issues and significant review finds each re-run the question with the affected people, because the duty tracks the issues as they evolve and knowledge as it accrues.

Unusual repositories matter

Adverse material distributes differently from helpful material. The sweep list, run deliberately against the data map:

- **Chat and messaging:** Teams and Slack threads, WhatsApp and Signal groups (work and, where used for work, personal), including reactions and edits; the single richest adverse stratum in modern disputes.
- **Drafts and the unsent:** draft folders, tracked-changes versions, comments and marginalia, the reply composed and abandoned; documents that say what the sent version was edited not to.
- **Voice and video:** voicemails, voice notes, recorded calls and meeting recordings with their auto-transcripts, which capture candour that writing filters.
- **Operational systems:** incident and complaint logs, quality and safety systems, ticketing queues, CRM notes: the places where the business recorded the problem as a problem, before anyone thought of litigation.
- **Oversight files:** internal audit reports, compliance reviews, board and committee packs, the internal investigation file (with its privilege status assessed deliberately, not assumed either way).
- **Personal corners:** OneNote and notebook apps, personal drives and cloud folders, "old laptop" archives, the individual's private paper trail kept precisely because something felt wrong.
- **The meta-repositories:** deletion and audit logs, retention-change histories and sync trails, which do not contain adverse documents but reveal where they were, and whose examination is forensic work when it matters.

The discipline is not to search all of this exhaustively in every case; it is to put each category consciously through the decision (search, sample, ask about, or record why not) so the certificate's confirmation covers the estate as it is, not the estate as filing conventions imagine it. The full source taxonomy and the interview questions that surface these locations are in *Finding the Evidence* and *The First eDisclosure Meeting*.

§ 0 8 · METHOD

The identification programme, step by step

STEP	ACTION AND OUTPUT
1 · Educate, in writing	The client letter explaining the duty in plain language (wording in §12), acknowledged; the anti-instinct inoculation, delivered before instinct acts
2 · Census the knowledge	List the people whose awareness counts (events and litigation-conduct), including leavers; owner and date per name
3 · Ask the adverse question	Census interviews with the direct question, safely framed; privileged notes with factual answers recorded; leaver outreach logged
4 · Design the search neutrally	Both-vocabulary terms, adverse coding in the protocol, TAR trained on relevance, escalation route live from day one of review
5 · Sweep the unusual repositories	Each §7 category through search / sample / ask / record-why-not, minuted against the data map
6 · Run the escalation log	Every flagged find assessed by supervising counsel within a set period; decisions (adverse or not, privilege, timing) recorded with reasons
7 · Disclose on the timetable	With Extended Disclosure or within the fallback timetable; late-arising knowledge disclosed promptly with a file note of the chronology
8 · Refresh on triggers	Amendments, witness statements, new custodians, significant finds: steps 2 to 5 re-run for the delta; certificate drafted, at the end, from this programme's records

Handling an adverse find

- **Stabilise.** No deletion, no "tidying", no forwarding around the business; the document and its source are preserved as found (forensically where integrity or completeness may be questioned), and the find enters the escalation log with its provenance.
- **Assess before adrenaline.** Is it actually adverse on the pleaded issues, or merely uncomfortable? Is it authentic, complete and in context (the full thread, the attachments, the later correction)? Half of feared documents shrink under sober reading; the other half need a strategy, not a reflex.
- **Check privilege precisely.** The underlying document is rarely privileged merely because it is damaging; advice about it is. Separate the two, and never let a privileged wrapper become a hiding place for a disclosable original.
- **Disclose on the clock, deliberately.** Within the applicable timetable, with the context that fairness allows (the surrounding thread, the correcting document), and with the client walked through why. A short internal note recording when the document became known and what was done closes the loop the certificate will rely on.
- **Fold it into strategy.** Adverse documents reshape merits honestly: settlement posture, witness handling, the framing of issues. The cases that end badly are almost never the ones with bad documents; they are the ones where bad documents met bad handling.

Worked examples

EXAMPLE 1 · THE INCIDENT LOG NOBODY CONNECTED

A manufacturer defended a defect claim on the basis that no comparable failures had occurred. The quality system, administered by a team never interviewed, held three incident tickets describing the same failure mode in other batches, entered months before proceedings. The tickets surfaced through a Model C request the claimant drafted from an industry-standard system name. The documents were survivable; the pleaded "no comparable failures", signed off without anyone asking the quality team the adverse question, was not. A step 2 census that included system owners, and a step 5 sweep of the operational systems, would have surfaced the tickets in week two and reshaped the Defence before it was served.

EXAMPLE 2 · THE LEAVER WHO ANSWERED HONESTLY

In a shareholder dispute, the leaver outreach (step 3) reached a departed finance manager with the standard question. She replied that a WhatsApp group, "Project Kestrel core", had discussed the disputed valuation in terms the company would not enjoy, and that she believed the group still existed on the two directors' phones. Targeted extraction recovered the thread intact; it was assessed, privilege-checked and disclosed with Extended Disclosure, accompanied by the later message in which the valuation approach was corrected. Painful, contextualised, and infinitely better than the alternative timeline in which the opponent's solicitors obtained the same thread from their own client's phone and led with the company's silence about it.

EXAMPLE 3 · TWO REVIEW ROOMS, ONE DOCUMENT

Identical fact pattern, two matters. A reviewer finds an internal email conceding the delay was "entirely our sequencing mess". In matter one, the protocol has an adverse code and a same-day escalation rule: counsel assesses it that afternoon, it is disclosed in the ordinary production, examined-in-chief on the client's terms at trial, and absorbed. In matter two, there is no adverse code; the reviewer tags it "relevant", it is produced unnoticed in a 9,000-document tranche, opposing counsel finds it, and the client first hears of its own email in cross-examination. Same document, same disclosure, entirely different cases: the difference was §5's coding rule and §8's log.

Common mistakes and technical limitations

Common mistakes

- **No client education**, so instinct ("we only hand over what helps") governs until it becomes conduct.
- **The unasked question**: interviews that map sources and chronology but never ask anyone, directly, about documents that hurt.
- **Advocate-built searches**: terms, coding and TAR training that could only ever return the party's own case.
- **No adverse code, no escalation route**: bad news seen in review and dissolved into "relevant".
- **Leavers skipped**, despite the duty expressly reaching their former awareness.
- **The operational systems ignored**: incident logs, complaints and audit files outside every search because they are not "documents" in anyone's mental model.
- **Privilege as camouflage**: disclosable originals withheld because advice about them was privileged.
- **Panic responses to finds**: deletion (spoliation plus the document), sitting on it (lateness compounding), or over-disclosure of half-understood material without assessment.
- **The one-time exercise**: the question asked in month one and never refreshed as issues, people and knowledge move.

Technical limitations

- **No system detects knowledge**. Search finds documents; only inquiry finds awareness. The census cannot be automated, and the certificate confirms a human process.
- **Absence is unprovable**. No methodology demonstrates that no adverse document exists; what can be demonstrated is that a proper inquiry was made, which is the standard the duty actually sets.
- **Materiality is judgment**. Adverse-or-not calls on marginal documents are legal assessments with reasons recorded, not coding-room votes; the log exists so the judgment is visible and consistent.
- **Recovery has limits**. Where the adverse document was deleted before contemplation under routine retention, recovery may be genuinely impossible; the examiner's evidenced statement of that fact (and of what the logs show about timing) is the honest, and protective, position.

§ 1 2 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Who had accountability for these events, and for this litigation, including people who have left? (This is the census list.)
- Has each of them been asked, directly, whether they are aware of any document that cuts against us? What did each say?
- Which systems recorded this subject-matter as a business problem (incidents, complaints, quality, audit), and who runs them?
- Is there anything you have been hoping we would not find? (Asked once, plainly, with the safety framing; the answer is privileged and the question has saved more clients than any other in this series.)

Ask your opponent

- Please confirm the steps taken to identify known adverse documents, including inquiries of former employees, and when they were performed.
- Your disclosure contains no material adverse to your case on issues [x, y]; please confirm the inquiry behind the certificate's confirmation.
- Please confirm whether your [incident / complaint / audit] systems were considered, and on what basis any were excluded.

Ask your eDiscovery / forensic provider

- How does the review protocol implement adverse coding and same-day escalation, and can we see the workflow and log format?
- How is TAR training audited against advocacy bias, and what QC sampling would show it?
- If an adverse document is (or may have been) deleted, what recovery and log analysis can you perform, and what evidenced statement results either way?

SUGGESTED WORDING · CLIENT LETTER PARAGRAPH (PLAIN-LANGUAGE EDUCATION)

"One duty requires special care. If you, or anyone who had responsibility for these events or for this dispute (including people who have since left), are aware of any document that harms our case or helps [opponent]'s on the issues (an email, a chat message, a note, a recording, an entry in any system), it must be disclosed. This applies even if no agreed search would ever find it, even where the court orders little or no other disclosure, and it continues until the case ends. If any such document comes to anyone's attention at any time, tell us immediately and take no other step: do not delete it, move it, or discuss it around the business. Documents of this kind, handled promptly and properly, are almost always manageable; concealed, they become the case. We will ask you and your colleagues about this directly, and we ask you to treat the question as the protection it is."

SUGGESTED WORDING · THE CENSUS INTERVIEW QUESTION (FOR THE NOTE)

"We are required to ask everyone with responsibility for these events the same question, and answering it fully protects you and the company: are you aware of any document, in any form or location (work or personal, formal or informal, current or deleted), that is inconsistent with the company's position on the issues in this dispute, or that you believe the other side would want to see? If you are unsure whether something counts, describe it and we will assess it; telling us about a document is never the wrong answer."

§ 13 · QUICK CONTROL

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

The known-adverse checklist

- ☐ Client educated in writing, acknowledgment on file, before instinct acts
- ☐ Knowledge census built: events people, litigation people, leavers, system owners
- ☐ The adverse question asked of each, directly and safely; answers recorded in privileged notes
- ☐ Leaver outreach performed and logged, engaged or not
- ☐ Search designed neutrally: both vocabularies, adverse coding, escalation route, TAR trained on relevance
- ☐ Unusual repositories each through search / sample / ask / record-why-not
- ☐ Escalation log live; every find assessed by counsel with reasons within the set period
- ☐ Finds privilege-checked precisely; originals never hidden behind advice
- ☐ Disclosure made on the applicable timetable, contextualised; late knowledge disclosed promptly with a chronology note
- ☐ Refresh triggers diarised (amendments, witness statements, major finds); certificate drafted from the programme's records

Red flags

- Any version of "we only disclose what helps us" surviving the first client meeting.
- A disclosure exercise, yours or theirs, whose productions contain nothing adverse at all.
- Interviews that mapped everything except the awkward question.
- A review protocol with no adverse code, or a log with no entries in a heavy case.
- Incident, complaint or audit systems absent from the data map.
- A find met with "let's think about whether this is really disclosable" stretching past the timetable.
- Deletion, settings changes or "tidying" anywhere near a known bad document.

When to involve a digital forensic expert

Four triggers in this territory. Where an adverse document is suspected but missing (the thread someone remembers, the log entry that should exist), examination of preserved sources, deletion artefacts and backups establishes what existed and what remains recoverable. Where a find's authenticity, completeness or chronology may be challenged (by either side), artefact-level analysis and a CPR Part 35 report settle it. Where deletion may have occurred after contemplation, log and artefact analysis dates it, which determines whether the problem is a document or spoliation. And where the informal repositories (handsets, chat apps, voice notes) must be swept properly, laboratory extraction is the precondition of an honest sweep. The wider escalation discipline is in *eDisclosure or Digital Forensics?*.

§ 1 4 · COMMON QUESTIONS

Frequently asked questions

What makes a document "adverse"?

It contradicts or materially damages your contended version of events on the issues in dispute, or supports your opponent's. The anchors are the pleaded issues and materiality: a document that is merely unflattering, or damaging on something not in issue, is not within the duty (though it may still fall within an ordered search). Marginal calls are legal judgments, made by counsel and recorded with reasons in the escalation log.

Whose knowledge counts as the company "knowing"?

People with accountability or responsibility for the events giving rise to the proceedings or for the conduct of the litigation, expressly including those who have left. Not every employee, and not the organisation in some abstract sense: the census exists to name the actual list, and reasonable inquiry of those people (leavers included) is how a company performs a duty framed around awareness.

Do we have to go looking for adverse documents?

The duty is framed around known documents, not a freestanding search obligation. But knowledge must be assembled honestly: asking the people whose awareness counts, running ordered searches neutrally, and not averting eyes from the obvious repositories. A party that structures its process to avoid acquiring knowledge invites the inference that it knew the knowledge was there to avoid, which is a worse position than the documents themselves.

What if the adverse document is privileged?

Genuinely privileged documents (legal advice, litigation work product) are not disclosable, adverse or otherwise, and the duty does not override privilege. The care point is precision: the damaging business document is not privileged because a lawyer later advised on it, and forwarding something to legal does not immunise it. Separate the original from the advice, take the decision deliberately, and record it.

We have just found something bad, late in the case. Now what?

Preserve it exactly as found, escalate to supervising counsel the same day, assess it soberly (authenticity, completeness, context, whether truly adverse), check privilege precisely, disclose promptly with such context as fairness allows, and record the chronology of when it became known and what was done. Late-arising knowledge, disclosed promptly, is the regime working; the only unrecoverable versions of this story involve delay or deletion.

How does this play in criminal and regulatory matters?

The same moral structure with sharper edges: CPIA 1996 obliges disclosure of material undermining the prosecution or assisting the defence, investigators must pursue reasonable lines of enquiry away from as well as toward a suspect, and regulators expect candour about damaging material in responses and self-reports. The three pillars translate directly, and the documentation habit (methodology described, inquiries logged) is if anything more valuable where the sanctions are personal.

§ 1 5 · REFERENCE

Glossary

Adverse code

The review-protocol designation for documents damaging to the producing party, with mandatory escalation.

Adverse document

A document contradicting or materially damaging a party's case, or supporting its opponent's, on the issues.

Census

The named list of people whose awareness counts for the company's knowledge, leavers included.

Escalation log

The dated record of flagged finds, counsel's assessments, privilege decisions and disclosure actions.

Knowledge refresh

Re-running the census and adverse question when issues, people or findings change.

Leaver outreach

Reasonable, recorded steps to put the adverse question to relevant former employees.

Neutral search design

Terms, coding and TAR training built to find damaging material as readily as supportive material.

Operational systems

Incident, complaint, quality, ticketing and audit systems: where the business recorded the problem as a problem.

Safety framing

Presenting the adverse question as protection, producing candour rather than defensiveness.

Unusual repositories

The informal and overlooked locations (chat, drafts, voice, personal notes, oversight files) where adverse material concentrates.

Wilful blindness

Structuring inquiry to avoid acquiring knowledge; the inference-generating pattern the programme exists to preclude.

CPIA test

The criminal disclosure standard: material undermining the prosecution case or assisting the defence.

Sources and authoritative references

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

- e-discovery.uk, EDRM Phase 05 · Review (audited review workflows, coding and QC: the machinery behind adverse coding and escalation) and Phase 04 · Processing (neutral, iterated term design with hit reports): e-discovery.uk/edrm/review · e-discovery.uk/edrm/processing
- e-discovery.uk, EDRM Phase 01 · Identification and the practice's method statement ("Bring us in early. Defensibility is built, not retrofitted"): e-discovery.uk/edrm/identification · e-discovery.uk
- cflab.uk, digital forensics services and deleted-data recovery (locating suspected-but-missing material, dating deletions from logs and artefacts, and CPR Part 35 reporting on authenticity and completeness): cflab.uk/digital-forensics-services
- cflab.uk, mobile phone forensics (the extraction behind an honest sweep of chat, voice notes and messaging apps): cflab.uk/mobile-phone-forensics · guides for lawyers: cflab.uk/guides
- Practice Direction 57AD (the duties, known adverse documents, timing and certification): justice.gov.uk, PD 57AD
- CPR Part 31 (standard disclosure's adverse-documents limb outside the B&PCs): justice.gov.uk, Part 31
- Criminal Procedure and Investigations Act 1996 and the Attorney General's Guidelines on Disclosure (rev. 2024): legislation.gov.uk/ukpga/1996/25 · gov.uk, AG's Guidelines
- CPR Part 35 (experts): justice.gov.uk, Part 35 · ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about the identification and disclosure of known adverse documents in the United Kingdom as at August 2026. The worked examples are fictional illustrations. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Rules and guidance change; always check the current text. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

The three pillars of this guide are services we run daily. Through **e-discovery.uk**: neutral search design tested against real data in both vocabularies, review workflows with adverse coding, same-day escalation and the audit log that later becomes the certificate's evidence, and TAR configured and QC-sampled for relevance rather than advocacy. Through the laboratory: the honest sweep of the informal estate (handsets, chat applications, voice notes) extracted completely under chain of custody; recovery and log analysis where an adverse document is suspected, missing or allegedly deleted, with the timing evidence that separates a bad document from spoliation; and authenticity, completeness and chronology examinations reported under CPR Part 35 / CrimPR Part 19 when a find is challenged. We also support the human pillar discreetly: examiners and consultants who join census interviews where technical follow-up questions land in real time. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine.



I N S T R U C T T H E L A B

Speak to a forensic examiner, not a salesperson.

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

NEW ENQUIRIES

+44 (0)20 7164 6971

EMAIL

info@cflab.uk

E-DISCOVERY

e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom

cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace