



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

A Privileged Document Has Been Disclosed: What Happens Next

The First Hours, the Legal Framework and the Recovery Playbook for Both Sides

It is Friday afternoon and someone has just realised: counsel's advice on the very issue in dispute went out in last month's production. Or the shoe is on the other foot: your reviewer has opened a document in the opponent's production that is plainly their QC's opinion. What happens in the next hours and days determines whether privilege survives, whether anyone can keep acting, and how much of the litigation budget the accident consumes. The law gives structure: CPR 31.20's permission requirement, the mistake-and-obviousness analysis the courts apply, clawback terms where the protocol has them, and injunctive relief where it has not. This guide is the playbook for both chairs: the disclosing party's immediate response and evidence-gathering, the receiving party's duties and dilemmas, the forensic work that establishes what happened and contains the spread, and the drafting that makes next time survivable. Guide 91 covers prevention; this is the aftermath.

⌚ Estimated reading time: 24 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**, has handled both chairs of inadvertent disclosure: the forensic reconstruction of how a document escaped, the containment and certified-deletion exercises that follow, and the workflow evidence that supports or resists relief: alongside the prevention machinery of guide 91 that makes the whole subject rarer.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

INCIDENT RECONSTRUCTION

CONTAINMENT & CERTIFIED DELETION

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

- 01 Executive summary
- 02 The problem in plain English: the document that got out
- 03 The legal framework: CPR 31.20, mistake, obviousness and clawback
- 04 The disclosing party's playbook: the first hours and the evidence
- 05 The receiving party's position: duties, dilemmas and safe handling
- 06 The forensic layer: reconstruction, containment and certified deletion
- 07 Consequences beyond the document: waiver reach, restraint and representation
- 08 Source architecture: where else the evidence lives
- 09 Worked examples
- 10 Common mistakes and technical limitations
- 11 Questions to ask · Suggested wording
- 12 Checklist and red flags · When to involve a digital forensic expert
- 13 Frequently asked questions
- 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: SPEED AND EVIDENCE DECIDE THESE INCIDENTS: THE DISCLOSING PARTY MOVES IN HOURS WITH A DOCUMENTED ACCOUNT OF THE MISTAKE; THE RECEIVING PARTY STOPS READING AND TAKES ADVICE; AND THE PROTOCOL DRAFTED LAST YEAR DOES MOST OF THE WORK

The framework in one paragraph: inspection happens; privilege is not automatically lost by an inadvertent production, but under **CPR 31.20** a receiving party may use a privileged document disclosed by mistake only with the court's permission: and the court's analysis asks whether there was a genuine mistake and whether it was obvious to the reasonable recipient (or the document was read before obviousness could bite), balancing the equities that injunction-style relief has always weighed. So the incident is fought on facts both sides start generating immediately. **Disclosing party:** notify fast and precisely (the document, the claim, the demand for non-use and return), gather the mistake evidence (guide 91 §5's review record showing the document was coded privileged, or how the workflow failed), and seek agreement or apply promptly: delay reads as acquiescence. **Receiving party:** the moment a document looks privileged, stop reading, quarantine it, take advice: use without permission risks injunctions, costs and, in bad cases, the removal of the litigation team that read too much. **Both:** the clawback terms of guide 91 §11: notice, non-use, return, no automatic waiver: convert most incidents into procedure instead of satellite litigation, which is why they were drafted before anyone needed them. The forensic layer (§6) reconstructs how the escape happened, contains the spread across the receiving estate, and certifies deletion: the technical closure the legal resolution depends on.

- **Hours matter:** notification and quarantine are same-day events: every day of silence weakens the claim and deepens the exposure.
- **The mistake is proved, not asserted:** the guide 91 review record is the disclosing party's best exhibit: or its absence, the receiving party's.
- **Reading is the risk:** the receiving team's exposure to content drives the remedies, including representation consequences: stop early, log exactly.
- **Clawback converts crisis to procedure:** protocol terms invoked beat applications launched: the drafting's payoff day.
- **Containment is technical:** copies spread through platforms, indexes and work product: the §6 sweep finds and certifies them all.

The problem in plain English: the document that got out

Large disclosure is a transfer of hundreds of thousands of documents under time pressure through human-and-machine pipelines: guide 91's prevention engineering reduces the escape rate and cannot make it zero. When an escape happens, the document is now inside the opponent's review platform, indexed, possibly read, possibly quoted in a memo: and the law must reconcile two principles that pull apart: privilege is fundamental and mistakes should not destroy it; but litigation runs on finality, and a party cannot unring every bell.

The reconciliation the courts have built is procedural and factual: use needs permission; permission turns on mistake and its obviousness; equity weighs conduct on both sides. Which means these incidents are won by whichever party behaves best and documents most from the first hour: the discloser who notifies same-day with the review record attached is in a different case from the one who noticed in March and wrote in June; the recipient who quarantined at paragraph two is in a different case from the one whose counsel's note quotes page four. This guide is the behaviour, both chairs, in order.

The legal framework: CPR 31.20, mistake, obviousness and clawback

- **CPR 31.20's gate:** where a party inadvertently allows a privileged document to be inspected, the inspecting party may use it or its contents only with the court's permission: the starting rule that makes unilateral use the dangerous move.
- **The mistake-and-obviousness analysis:** the courts' approach (in the *Al-Fayed* line and its successors) asks whether inspection was permitted by mistake and whether that would have been obvious to the reasonable solicitor: with obviousness, actual appreciation, and what was read before realisation all in the balance: fact questions the §4-§6 records answer.
- **Equitable roots and remedies:** behind the rule sits confidence-based injunctive relief: restraint of use, delivery up, and in serious cases consequences for the legal team exposed: discretionary, conduct-sensitive, and prompt is stronger.
- **Clawback by agreement:** protocol terms (guide 91 §11's paragraph) making notice, non-use, return and no-automatic-waiver the contractual default: the machinery most incidents now resolve through, PD 57AD's cooperation culture supporting it.
- **Waiver's separate track:** inadvertent production is analysed differently from deliberate deployment (guide 91 §7): but sloppiness at scale, repeated escapes, or delay can push an incident toward loss of privilege: the framework protects the careful, not the careless.

The disclosing party's playbook: the first hours and the evidence

- **Confirm and scope, immediately:** what exactly went out: the document, its family, its duplicates and thread instances (guide 82-83's structures searched at once): one escaped hop often means siblings escaped too: the full escape list before the letter, or the letter amended twice.
- **Notify the same day:** identify the document(s) by production number, assert the claim and its basis, state the mistake, demand quarantine, non-use and return or certified deletion, and invoke the clawback clause: precise, prompt, unapologetic: the template of §11 exists for this hour.
- **Assemble the mistake evidence:** the guide 91 §5 review record (the document coded privileged; the production error that overrode it), the QC records, the workflow account: mistake proved from files, per the standing record-keeping principle: this is the exhibit the application stands on.
- **Escalate on the clock:** agreement sought first; the application issued promptly where refused or ignored: delay is the discloser's own worst evidence.
- **Fix the pipeline in parallel:** the escape's cause corrected and documented (the guide 91 §6 sweep tightened): both because the court will ask, and because the second escape is the one that loses the privilege.

The receiving party's position: duties, dilemmas and safe handling

- **Recognise and stop:** the reviewer's trigger list (counsel's opinions, advice headers, lawyer-to-client traffic on the issues): reading stops at recognition, the exposure logged (who, what, how far): the log that later shows restraint.
- **Quarantine technically:** the document sequestered from the review workspace: coding frozen, access restricted, downstream copies (work product, memos, exports) identified: §6's containment run on your own estate.
- **Notify or respond properly:** under clawback terms, notice flows and the machinery runs; absent terms, the safe course is prompt engagement with the discloser's claim rather than quiet use: CPR 31.20 makes unilateral deployment the position of maximum risk.
- **The dilemma handled honestly:** where the receiving party believes the document was not privileged, or the mistake not obvious, that is argued with the document quarantined: the contest is for the court, not for the review team's ongoing reading.
- **Protect the team:** exposure minimised and recorded because representation challenges follow deep exposure in serious cases: the firm that can show two paragraphs and a stop is safe; the one whose strategy memo quotes the advice is not.

The forensic layer: reconstruction, containment and certified deletion

- **Escape reconstruction:** how the document left: the coding history, the production-set assembly, the override or QC gap: rebuilt from platform audit trails (guide 91 §5's biography) into the §4 mistake evidence: the workflow's black box read after the incident.
- **Spread mapping:** where the document now lives in the receiving estate: review platform instances, indexes and search caches, exports, work product, emails quoting it: the guide 82 §7 hash-hunt run across the recipient's environment, cooperatively or under order.
- **Containment and deletion:** instances removed or sequestered, indexes purged, work product addressed per the agreed or ordered terms: with the practical honesty that platform architectures complicate perfect deletion: what was done, where residuals persist and why, stated plainly.
- **Certification:** the deletion certificate: instances found, actions taken, by whom, verified how: the document that closes the incident, credible because a named specialist signs it.
- **Neutral roles:** on contested incidents, an independent forensic party can run the sweep and certify across both estates: the guide 71 §7 agreed-specialist pattern, applied to cleanup.

Consequences beyond the document: waiver reach, restraint and representation

- **Waiver reach contested:** the receiving party may argue loss of privilege in the document or its subject matter: resisted with the §4 evidence and the clawback terms' no-automatic-waiver language: the drafting doing exactly what it was drafted for.
- **Restraint and use injunctions:** orders preventing deployment of the content, striking references from statements of case or evidence, and policing derivative use: the remedies that make early quarantine the receiving party's cheapest option in hindsight.
- **Representation consequences:** in serious exposure cases, applications to restrain the exposed legal team from continuing to act: rare, grave, and driven by the exposure log's contents: §5's minimisation discipline priced accordingly.
- **Costs follow conduct:** the party that behaved and documented well recovers; the party that delayed, read on, or resisted obviousness pays: the incident's whole economics tilting on the first week's behaviour.
- **Regulatory and client dimensions:** serious escapes engage professional duties, client notification and, where personal data is involved, breach-assessment questions: managed alongside, not after, the litigation response.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: an inadvertent-disclosure incident is decided on evidence that already exists in identifiable places, and both chairs assemble from the same map. The incident's facts live in: the review and production records (the document's coding history, the QC runs, the set-assembly logs: mistake proved or disproved from the guide 91 biography); the production artefacts themselves (load files, indexes and exchange records dating exactly what left, when); the receiving estate (platform access logs showing who opened the document and for how long: the exposure question answered from telemetry, not recollection); the correspondence record (notice timing, responses, the conduct chronology both judgments and costs orders read); the spread map (§6's hash-hunt results: instances, copies, work product); and the protocol (the clawback terms that either exist and govern, or do not and are missed). Neither chair should assert what these sources can prove: the incident's entire litigation is an exercise in reading them fast and first.

QUESTION	REVIEW & PRODUCTION RECORDS	PRODUCTION ARTEFACTS	RECEIVING-ESTATE TELEMETRY	CORRESPONDENCE RECORD	SPREAD MAP	PROTOCOL TERMS
Was it a mistake?	Y: the coding history	Set assembly logs	n/a	Consistent prior claims	n/a	n/a
Was it obvious?	The document's face	Context in the production	Reading behaviour	What recipient said when	n/a	Notice standards
Who read what?	n/a	n/a	Y: access logs + durations	The exposure log	Work-product citations	n/a
Who behaved well?	Pipeline fix evidence	n/a	Quarantine timing	Y: the conduct chronology	Cooperation with sweep	Terms invoked or ignored
Is it contained?	n/a	Index purge records	Deletion verification	n/a	Y: the certificate's basis	Return/destroy machinery

Fallback strategy in one line: both chairs win or lose on records: the discloser's workflow biography, the recipient's exposure telemetry, the correspondence clock: read them first, assert second.

Worked examples

EXAMPLE 1 · THE FRIDAY DISCOVERY, RUN BY THE BOOK

A junior reviewer, re-checking a coding query, realised counsel's advice on limitation: coded privileged in March: had gone out in the May production: a set-assembly filter had used a stale saved search predating the privilege overlay. Within four hours: the guide 82-83 sweep found the escape was three instances (the email and two thread copies); the §11 notice went out identifying all three by production number, invoking the protocol's clawback clause; and the platform's audit export proving the March coding was attached. The receiving party confirmed quarantine the same evening: their own access logs showed one reviewer had opened the lead document for forty seconds. Certified deletion followed within the week under the §6 machinery, the pipeline defect was fixed and documented, and the incident never reached the court. Total cost: a bad Friday. The counterfactual runs through every following section.

EXAMPLE 2 · THE RECIPIENT WHO READ ON

A claimant's team, reviewing a defendant production, opened a document headed with a law firm's name and the subject "Advice: prospects and settlement strategy": and read it, circulated it internally, and built a strategy note quoting its assessment of the defendant's weaknesses. When the defendant's notice arrived nine days later, the claimant resisted: no obvious mistake, privilege lost. The application went badly: the court found the mistake obvious to a reasonable solicitor on the document's face; permission to use was refused; the strategy note and its derivatives were ordered delivered up; and: the part that made the law reports: the two lawyers with deep exposure were restrained from further conduct of the limitation issue, with the costs of the reconstituted team's reading-in falling on the claimant. The forty-second reviewer of Example 1 and this team read the same kind of document; the difference was everything after recognition.

EXAMPLE 3 · THE CONTESTED CLAIM, RESOLVED ON THE RECORD

A discloser demanded return of an "inadvertently produced privileged" board pack extract; the recipient, before quarantining, had seen enough to doubt the claim: the extract looked like commercial analysis, not advice. The dispute resolved the §8 way: the recipient quarantined and contested rather than used; the discloser's review record, produced on the application, showed the extract had been coded "not privileged" by two reviewers and swept into the claim only by a post-production keyword panic; and the underlying document, examined by the court, contained no legal advice. The claim failed: not because a mistake was impossible, but because the discloser's own biography contradicted it. Costs followed. The example's two lessons run both directions: recipients who quarantine-and-contest lose nothing by the discipline; and disclosers' clawback demands are exhibits: made only where the record supports them.

Common mistakes and technical limitations

Common mistakes

- **Delay on discovery:** the escape noticed and sat on: acquiescence built into the discloser's own chronology.
- **Reading past recognition:** Example 2's team: exposure deepened when the duty was to stop.
- **Notices without scope:** the lead document demanded back while its thread copies and duplicates sit unmentioned: the §4 sweep skipped, the letter amended twice.
- **Unilateral use:** CPR 31.20 bypassed on self-assessed confidence: the maximum-risk posture, chosen voluntarily.
- **Clawback terms never drafted:** the incident arriving on a protocol that says nothing: guide 91 §11's paragraph, missed when it was cheap.
- **Mistake asserted without the record:** Example 3's discloser: the claim contradicted by its own biography.
- **Containment declared, not verified:** "we deleted it" without the sweep, the indexes, or the certificate: residual copies surfacing later at the worst price.
- **The pipeline left unfixed:** the same defect escaping twice: the second incident meeting a much colder court.

Technical limitations

- **Perfect deletion is architectural fiction:** platforms cache, index and back up: certificates state what was done and what persists where, honestly: credibility over cosmetics.
- **Exposure telemetry varies:** access logs differ by platform in depth and retention: the exposure question answered as well as the telemetry allows, with gaps stated.
- **Spread outpaces recall:** exports, printouts and quoted fragments travel beyond any sweep's certainty: containment bounded honestly, per the standing rule.
- **Obviousness is judged on the face:** no forensic exercise substitutes for the document reading as what it is: the analysis stays legal at its core.
- **Cross-border recipients complicate remedies:** foreign teams and platforms stretch enforcement: the practical reach mapped before the demand promises it.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client (as discloser)

- Is the escape list complete: the document, its family, duplicates, thread instances: before the notice commits us?
- What does the review record actually show for these documents: and does it prove the mistake or embarrass the claim?
- What was the pipeline defect, and is it fixed and documented before the court asks?

Ask your opponent (as recipient, or of a recipient)

- Please confirm quarantine of [documents], identifying by name and role each person who has accessed them, the extent of any reading, and all copies, exports or work product referring to their contents.
- Please confirm return or certified deletion of all instances in accordance with [the protocol / CPR 31.20], including removal from review platforms, indexes and derivative materials, with a certificate of the steps taken.
- (As recipient, of a discloser:) Please provide the basis on which the material is said to be privileged and to have been produced by mistake, including the relevant review and production records.

Ask your eDiscovery / forensic provider

- What do the platform audit trails show about how this escaped: and how fast can the mistake evidence be exported?
- What is the spread map in the receiving estate: instances, indexes, work product: and what will certified deletion actually cover?
- What does our own exposure telemetry show, person by person, if we are the recipient?

SUGGESTED WORDING · SAME-DAY NOTICE OF INADVERTENT DISCLOSURE

"We write further to our production of [date]. The documents identified in the schedule to this letter are subject to [legal advice / litigation] privilege and were produced as a result of an inadvertent error in the assembly of the production set, notwithstanding their identification as privileged in our review, as our contemporaneous records confirm. Pursuant to [paragraph X of the protocol / CPR 31.20], we require that you and all persons with access: (1) immediately cease any reading, use or copying of the documents; (2) quarantine all instances, including within any review platform, index or derivative work product; (3) confirm by [time/date] the identity of any person who has accessed them and the extent of such access; and (4) return or certify deletion of all instances within [7] days. This disclosure was inadvertent and does not constitute a waiver of privilege in the documents or their subject matter. We reserve all rights, including to apply without further notice if the above is not confirmed."

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

The incident checklist (both chairs)

- ☐ Escape scoped across duplicates, families and threads before the notice
- ☐ Same-day notice sent: precise, clause-invoking, rights-reserving
- ☐ Mistake evidence exported from the review record immediately
- ☐ Recipient: reading stopped at recognition; exposure logged
- ☐ Recipient: quarantine executed technically, not just declared
- ☐ Spread map built; containment run; residuals stated honestly
- ☐ Certified deletion documented by a named specialist
- ☐ Pipeline defect fixed and the fix documented
- ☐ Conduct chronology maintained from hour one
- ☐ Clawback terms in every protocol going forward: guide 91 §11

Red flags

- Notices sent weeks after discovery: the discloser's own worst exhibit.
- Strategy documents quoting the opponent's advice: Example 2's gravity.
- Clawback demands unsupported by the review record: Example 3's collapse.
- "Deleted" without a sweep, an index purge, or a certificate.
- Repeat escapes from the same unfixed pipeline.
- Exposure accounts from memory where telemetry exists.
- Protocols still silent on inadvertent disclosure.

When to involve a digital forensic expert

Immediately, in either chair: on the disclosing side, to scope the escape, export the mistake evidence and fix the pipeline (Example 1's four hours); on the receiving side, to quarantine technically, read the exposure telemetry and run containment credibly; on contested incidents, as the neutral running the sweep and certifying deletion across both estates; and on applications, evidencing workflow, exposure and containment under CPR Part 35. Through **e-discovery.uk**, the prevention machinery of guide 91 and the response machinery of this guide are the same team: which is the cheapest fact in the whole subject.

§ 13 · COMMON QUESTIONS

Frequently asked questions

Is privilege automatically lost once the document has been produced?

No: inadvertent production does not of itself destroy privilege, and CPR 31.20 bars the recipient's use without permission: the analysis then turning on mistake, obviousness and conduct. What erodes protection is behaviour: delay, repeat escapes, resistance to the machinery: the framework protects the careful.

We are the recipient and the document looks privileged. Must we really stop reading?

Yes, at recognition: further reading deepens exposure that drives every remedy, up to representation consequences in serious cases: Example 2 is the standing illustration. Stopping costs nothing: if the claim fails (Example 3), the quarantined document returns to the review untouched by your restraint.

What if we genuinely think the document is not privileged, or the mistake was not obvious?

Quarantine and contest: the argument is made to the court with the document sequestered, not resolved by continuing to read: the recipient who does this loses nothing by the discipline and, where right, wins with clean hands: Example 3's path. Unilateral use on self-assessment is the one position that can convert a good argument into a bad outcome.

How fast does the disclosing party need to move?

Same day for the notice once the escape is confirmed, days not weeks for the application if the machinery stalls: delay reads as acquiescence and is the single most common self-inflicted wound. The speed is achievable precisely because the evidence is exportable: Example 1's four hours were mostly the sweep, not the drafting.

Can deletion from the opponent's systems ever really be verified?

To a credible, stated standard: instances found by hash-sweep, removed or sequestered, indexes purged, work product addressed, residual architecture (backups, caches) disclosed honestly: the certificate describing exactly that, signed by a named specialist. Perfect erasure is not the promise; documented, verified containment is: and courts accept the honest version over the cosmetic one.

Does one inadvertent disclosure waive privilege over the whole subject matter?

Not of itself: the clawback language and the case law both resist subject-matter waiver from genuine accidents promptly handled: the collateral-waiver risks live mainly in deliberate deployment (guide 91 §7) and in conduct that stops looking accidental: repeat escapes, knowing silence, selective assertion. Handle the incident by this guide and the document, not the privilege, is what needs recovering.

§ 1 4 · REFERENCE

Glossary

Certified deletion

Documented, specialist-verified removal of escaped instances.

Clawback

Agreed notice-and-return terms for inadvertent disclosure.

Containment

Finding and neutralising every copy in the receiving estate.

CPR 31.20

The permission requirement for using inadvertently inspected privileged material.

Delivery up

The remedy returning or destroying material and derivatives.

Exposure log

The record of who read what, how far, when.

Mistake evidence

The review-record proof that production was in error.

Obviousness

Whether the mistake was apparent to the reasonable recipient.

Quarantine

Technical sequestration from review, indexes and use.

Spread map

The hash-hunt census of where the document now lives.

Sources and authoritative references

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

- cflab.uk, digital forensics services (incident reconstruction, containment sweeps, certified deletion, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 05 · Review and Phase 06 · Production (the workflow records and QC gates the incident analysis reads): e-discovery.uk/edrm/review · e-discovery.uk/edrm/production
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- CPR Part 31, r.31.20: [justice.gov.uk](https://www.justice.gov.uk/courts/procedure-rules/civil/part31), Part 31 · PD 57AD: [justice.gov.uk](https://www.justice.gov.uk/courts/procedure-rules/civil/part31), PD 57AD
- *Al-Fayed v Commissioner of Police of the Metropolis* [2002] EWCA Civ 780 (the mistake-and-obviousness principles): [bailii.org](https://www.bailii.org/uk/other/ewca/cases/index.html), *Al-Fayed*
- CPR Part 35: [justice.gov.uk](https://www.justice.gov.uk/courts/procedure-rules/civil/part35), Part 35 · ICO, UK GDPR guidance (personal-data dimensions of escapes): ico.org.uk

DISCLAIMER

This publication provides general information about inadvertent disclosure of privileged material as at August 2026. The law in this area is discretionary and intensely fact-specific; nothing here substitutes for advice on a live incident, which should be sought immediately. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

Incident work at the laboratory runs both chairs at incident speed: on the disclosing side, the escape scoped across duplicates and threads within hours, the mistake evidence exported from the platform's audit trails, the pipeline defect found and fixed (Example 1's afternoon); on the receiving side, technical quarantine, exposure telemetry read person by person, and containment that will bear a certificate; and on contested incidents, the neutral-specialist role: sweeping, certifying and reporting under CPR Part 35 across both estates. Behind it sits guide 91's prevention machinery through **e-discovery.uk**: the pre-production sweeps and clawback drafting that make this guide's subject rare. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if the bad Friday is happening right now, the first hour's calls are the sweep and the notice: in that order, today.



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