How To Build A Defensible EDisclosure Strategy At The Start Of A Case

Building a defensible eDisclosure strategy is crucial for UK litigators. This guide details the ten steps, from day-one preservation and data mapping to search design and review protocols, ensuring a robust and compliant approach to electronic disclosure.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-29.
https://e-discovery.uk/library/how-to-build-a-defensible-edisclosure-strategy-at-the-start-of-a-case

EDISCLOSURE STRATEGY · A GUIDE FOR UK LAWYERS How to Build a Defensible e Disclosure Strategy at the Start of a Case From Pleadings and Issues to Collection and Review Protocols COMPUTER FORENSICS LAB DISCOVERY. UK

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: strategy or improvisation 03 Why the first weeks matter legally 04 The workflow at a glance 05 Step 1 · Pleadings to issues: the issue-source matrix 06 Step 2 · Day-one preservation 07 Step 3 · Identification: the data map 08 Step 4 · Custodian selection and tiering 09 Step 5 · Control analysis and third parties 10 Step 6 · Forensic triage 11 Step 7 · Early data assessment 12 Step 8 · Search design 13 Step 9 · The procedural position: DRD, Models, budget 14 Step 10 · Collection plan and review protocol 15 The strategy document and its governance 16 Common mistakes and technical limitations 17 Questions to ask · Suggested wording for instructions 18 Checklist and red flags · When to involve a digital forensic expert 19 Frequently asked questions 20 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: WHAT MAKE SA STRATEGY DEFENSIBLE

§ 02 · FIRST PRINCIPLES The problem in plain English: strategy or improvisation

§ 03 · WHYITMATTERSLEGALLY Why the first weeks matter legally

§ 04 · THEMAP The workflow at a glance TRIAGE DESIGN BUDGET REVIEW PROTOCOLS WHEN WHAT IS DONE WHAT EXISTS AT THE END

§ 05 · STEP1 Pleadings to issues: the issue-source matrix

§ 06 · STEP2 Day-one preservation

§ 07 · STEP3 Identification: the data map

§ 08 · STEP4 Custodian selection and tiering

§ 09 · STEP5 Control analysis and third parties

§ 10 · STEP6 Forensic triage

§ 11 · STEP7 Early data assessment

§ 12 · STEP8 Search design

§ 13 · STEP9 The procedural position: DRD, Models, budget CMC.

§ 14 · STEP10 Collection plan and review protocol

§ 15 · THEARTEFACT The strategy document and its governance SECTION CONTENTS (THE STEP OUTPUTS, FILED ONCE) 1 · Issues Working Issues for Disclosure; the issue-source matrix; date anchors 2 · Preservation Hold notice and register; suspensions; third-party and leaver notices; client 3 · Sources Data map (versioned); questionnaire returns; cross-check results 4 · Custodians Tiered list with rationales; identity tables; system owners; interview records 5 · Control Control schedule; requests and notices with responses; third-party route plan 6 · Forensic Triage record; acquisition logs; the escalation protocol; exam in at i on scopes 7 · Assessment The assessment report and scenario models 8 · Search Search protocol; term proposals and hit reports; validation plan 9 · Procedure DRD / EDQ drafts and annexes; budget alignment; negotiation brief 10 · Execution Collection plan; review protocol; production specification; provider instructions

§ 16 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 17 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording for instructions Ask your client, on day one Ask your opponent, through the process Ask an e Discovery / forensic provider, at engagement SUGGESTED WORDING · ENGAGEMENT INSTRUCTION TO A PROVIDER (CORE PA R AG RAPHS) ANDCASEPLAN)

§ 18 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The strategy checklist Red flags When to involve a digital forensic expert

§ 19 · COMMON QUESTIONS Frequently asked questions What makes an e Disclosure strategy "defensible"? How early is early? The dispute has only just surfaced. 3 to 6 belong in the first fortnight even pre-action: preservation duties are live, pre-action protocols reward Our client already collected data themselves. Is the strategy compromised? Does a small case need all ten steps? What happens to the strategy when the case changes? Who should build the strategy: the firm, the client or the provider?

§ 20 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

What makes an e Disclosure strategy "defensible"?

Three properties. Connection: every scope and method decision traces to the pleaded issues through the matrix, the tiering and the protocol. Evidence: decisions rest on measured numbers and tested terms, not instinct. Records: the strategy generates its documents as it executes (hold register, data map, control schedule, assessment report, search protocol, logs), so any later challenge is answered by production, not reconstruction. A strategy with those properties can be wrong in places and still defensible; a strategy without them can be right every where and still in defensible. How early is early? The dispute has only just surfaced. Step 2 is due the day proceedings are contemplated, which is usually before anyone calls it litigation. Steps 1 and 3 to 6 belong in the first fortnight even pre-action: preservation duties are live, pre-action protocols reward preparedness, and pre-action assessment (Step 7) improves pleading and settlement judgment. Nothing in the workflow waits for issue of proceedings; the CMC merely collects its outputs.

Our client already collected data themselves. Is the strategy compromised?

Damaged, not doomed. Record exactly what was done, by whom, when and with what tools; stop further self- help immediately; assess with the provider what the in form a l collection preserved and destroyed; re-collect defensibly where sources still allow it; and route anything trigger-positive to forensic assessment of the handling itself. Candour in the DRD about the early handling, with the remediation documented, is a survivable position; discovery of it by the opponent is not.

Does a small case need all ten steps?

It needs all ten questions answered; the answers are just shorter. A two-custodian employment dispute can run Step 2 in an after no on, Steps 3 to 6 in two meetings, Step 7 at level 1 only, and Steps 8 to 10 in a five-page protocol. What small cases cannot safely skip is the same as large ones: day-one preservation, reasoned scope, tested terms and a written record.

What happens to the strategy when the case changes?

It versions. Amended pleadings re-run Step 1's matrix; new custodians re-run Steps 4 to 6 for the additions; staged tranches promote on their defined triggers; and each change is dated and reasoned in the document. The living-document commitment belongs in the DRD itself, because promptly proposed, well-recorded changes read as diligence while silent ones read as concealment.

Who should build the strategy: the firm, the client or the provider?

The firm owns it (the certificate and the court-facing assertions are the lawyers'); the client supplies the facts and a single accountable IT channel; the provider contributes the measurement, the technical constraints and the execution machinery, and a good one will challenge the plan where the estate cannot support it. What fails is delegation of the whole to either of the other two: client-built strategies inherit self-collection risks, and provider- built ones optimise for workflow rather than for the case. cflab. u k · e-disc ove r y. u k