# Preparing A Forensic Collection Protocol

A forensic collection protocol is a written plan ensuring defensible data collection. This guide details its anatomy, covering scope, exclusions, execution, and contingencies, and provides guidance on drafting and agreement for UK legal professionals.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/preparing-a-forensic-collection-protocol

COLLECTION PROTOCOL S · A GUIDE FOR UK LAWYERS Preparing a Forensic Collection Protocol The Written Plan That Makes a Collection Defensible Before It Begins COMPUTER FORENSICS LAB DISCOVERY. UK

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES PROTOCOL DRAFTING & EXECUTION CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: collections without plans 03 What a protocol is, and when one is needed 04 The anatomy: section by section 05 Scope: custodians, sources, date ranges, method per source 06 Exclusions, privilege and personal data 07 Execution: sequence, roles, verification and custody 08 Contingencies and escalation triggers 09 Agreed and court-ordered protocols 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

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: WRITETHECOLLECTIONDOWNBEFOREITHAPPENS

§ 02 · FIRST PRINCIPLES The problem in plain English: collections without plans

§ 03 · DEFINITION What a protocol is, and when one is needed

§ 04 · THESKELETON The anatomy: section by section SECTION CONTENTS 1 · Purpose and authority The matter, the legal basis (instruction, order, consent), the protocol's status and version, 2 · Scope Custodians (Schedule A), sources (Schedule B), date ranges, data types in and out 4 · Exclusions and privilege What is not collected; how privileged and personal material encountered is handled; review 5 · Execution plan Sequence, sites, dates, roles (examiner, IT, supervising lawyer), powered-on device 6 · Verification and custody Hashing standards, acquisition records, exhibit referencing, sealing, storage and transfer 7 · Contingencies Encryption without credentials, absent or failed devices, unexpected sources, refusals, 8 · Escalation triggers Discoveries that pause execution and refer back: suspected deletion, contested material, 9 · Deliverables and What the exercise produces: evidence schedule, hash schedule, deviation log, collection 10 · Amendment How the protocol changes: written variation, logged, approved by the named owners

§ 05 · SCOPE Scope: custodians, sources, date ranges, method per source

§ 06 · THESENSITIVEMATERIAL Exclusions, privilege and personal data

§ 07 · EXECUTION Execution: sequence, roles, verification and custody

§ 08 · WHENREALITYINTERVENES Contingencies and escalation triggers

§ 09 · TWO - PARTY PROTOCOL S Agreed and court-ordered protocols

§ 10 · IN THE WILD Worked examples EXAMPLE1 · THECORRIDORDECISION EXAMPLE2 · THEPROTOCOLANNEXEDTOTHEORDER EXAMPLE3 · THEHYBRIDTHATSTAYEDDEFENSIBLE

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

§ 12 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · PROTOCOLCORECLAUSES ( A DA PT ) SUGGESTED WORDING · C OV ERLETTERE XC HANGINGTHEPROTOCOL

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

§ 14 · COMMON QUESTIONS Frequently asked questions Is a protocol really necessary for a small, single-device matter? Should we show our collection protocol to the other side? What is the difference between the collection protocol and the DRD's methodology sections? Can the client's IT team execute parts of the protocol to save cost? What happens when execution has to depart from the protocol? Who signs off the protocol, and does the client need to?

§ 15 · 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

**Is a protocol really necessary for a small, single-device matter?**

At one page, yes: source, method, hashing, custody, the encryption contingency, and who decides surprises. The habit standardises quality, the page takes twenty minutes, and small matters have a way of growing: the one- page protocol from month one reads very well in the witness box of month eighteen. What scales with matter size is the document's depth, never the existence of the discipline.

**Should we show our collection protocol to the other side?**

Usually, and often before execution: methodology is process-plane material (per this series' cooperation guide), exchanging it forecloses later disputes cheaply, and the cover letter's "observations before execution rather than after" framing shifts the burden of silence onto them. Hold back only genuinely strategic elements (which sources you consider contested, escalation reasoning that reveals theory), which belong in a privileged annex rather than the exchanged body.

**What is the difference between the collection protocol and the DRD's methodology sections?**

Sequence and status: the protocol is the operational instrument, written first, at full technical depth, and executed against; the DRD summarises it for the court at the level PD 57AD requires. Writing the protocol first means the DRD reports a designed exercise rather than promising an undesigned one, and when the DRD is questioned, the protocol and its execution record are the annexes that answer.

**Can the client's IT team execute parts of the protocol to save cost?**

Yes, under the hybrid conditions of Example 3: examiner-written per-source methods, training and a supervised first run, provided verification tooling, manifests, sample re-collection, and daily deviation reporting. Without those, in-house collection is the cheapest way to buy the most expensive problem; with them, it is a legitimate proportionality tool the protocol makes visible and defensible.

**What happens when execution has to depart from the protocol?**

It departs, in the open: the deviation is logged (what, why, who decided, when), material departures are made as amendments approved by the named owners, and the collection report reconciles plan against execution including every delta. Deviations are expected and survivable; drift is not: the difference is whether the departure has an entry, a decider and a reason, or is discovered by comparison two years later.

**Who signs off the protocol, and does the client need to?**

The instructing lawyer (scope, privilege, legal basis) and the executing examiner (method, feasibility) must; the client signs where its people perform steps, where business disruption is authorised, or where the protocol embodies its UK GDPR decisions, which in corporate collections it usually does. Signature blocks are not ceremony: they are the answer, two years on, to "who approved this?", and the protocol exists to make that answer boring. cflab. u k · e-disc ove r y. u k 