

What Is A Reasonable Electronic Search

Understanding a reasonable electronic search is crucial for UK litigators. This guide details the levers involved, such as custodians, dates, keywords, and analytics, alongside the legal standards of CPR 31.7, PD 31B, and PD 57AD, to ensure defensibility and avoid common pitfalls.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-29.
<https://e-discovery.uk/library/what-is-a-reasonable-electronic-search>

THEREASONABLESEARCH · A GUIDE FOR UK LAWYERS What Is a Reasonable Electronic Search? Custodians, Dates, Keywords, Analytics and Defensibility COMPUTER FORENSICS LAB DISCOVERY. UK

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES SEARCH-TERM NEGOTIATION
SUPPORT TAR / CAL WITH STATISTICAL VALIDATION FULL CHAIN-OF-CUSTODY
DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: two ways to fail 03 The legal standard: CPR 31.7, PD 31B and PD 57AD 04 Lever 1 · Custodians 05 Lever 2 · Date ranges 06 Lever 3 · Sources 07 Lever 4 · Keywords 08 Lever 5 · Analytics and technology-assisted review 09 Lever 6 · Proportionality 10 Lever 7 · Sampling and validation 11 Worked examples: the overly narrow search 12 Worked examples: the excessively broad search 13 Defensibility: the paper trail behind the search 14 Negotiating search terms with the other side 15 Common mistakes and technical limitations 16 Questions to ask · Suggested wording for instructions 17 Checklist and red flags · When to involve a digital forensic expert 18 Frequently asked questions 19 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE ANSWER:
WHATISAREASONABLESEARCH?

§ 02 · FIRST PRINCIPLES The problem in plain English: two ways to fail THE KEYHOLE (OVERLY NARROW) THE LANDSLIDE (EXCESSIVELY BROAD)

§ 03 · THELAW The legal standard: CPR 31.7, PD 31B and PD 57AD FOR THE PRACTITIONER

§ 04 · LEVER1 Custodians

§ 05 · LEVER2 Date ranges

§ 06 · LEVER3 Sources

§ 07 · LEVER4 Keywords

§ 08 · LEVER5 Analytics and technology-assisted review

§ 09 · LEVER6 Proportionality

§ 10 · LEVER7 Sampling and validation

§ 11 · IN THE WILD Worked examples: the overly narrow search EXAMPLE1 ·
THEPLEADINGSVOCABULARYTRAP EXAMPLE2 ·
THERANGETHATSTARTEDATTHECONTRACT EXAMPLE3 · THEMISSINGCHANNEL

§ 12 · IN THE WILD Worked examples: the excessively broad search EXAMPLE1 ·
THESINGLE - WORDTERMLIST EXAMPLE2 · RESTOREEVERYTHING, JUST IN CASE
EXAMPLE3 · EVERY ON E, TOBESAFE

§ 13 · THEPAPERTRAIL Defensibility: the paper trail behind the search DOCUMENT WHAT IT
RECORDS

§ 14 · ACROSS THE TABLE Negotiating search terms with the other side

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

§ 16 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording for
instructions Ask your client Ask your opponent Ask an e Discovery provider SUGGESTED
WORDING · SEARCHPROTOCOLPREAMBLE (CORE PA R AG RAPHS) SUGGESTED
WORDING · PROPOSINGTERMSTOTHEOTHERSIDE

§ 17 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The
reasonable-search checklist Red flags When to involve a digital forensic expert

§ 18 · COMMON QUESTIONS Frequently asked questions What is a reasonable electronic
search? Do we have to search backups? Can we rely on keywords alone? Are we required to
use TAR? A relevant document has surfaced that our search never caught. Is the certificate
wrong? Who decides if the parties cannot agree terms?

§ 19 · REFERENCE Glossary TAR 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 is a reasonable electronic search?

One whose scope and method are rationally connected to the issues, proportionate under the CPR 31.7 and PD 31B factors, tested against the data (sampled terms, validated stopping points) and documented so its description in the disclosure statement or DRD is accurate and its limits are stated. It is a standard of process, not of perfection: relevant documents can be missed by a reasonable search, and unreasonable searches can fail in either direction, keyhole or landslide.

Do we have to search backups?

You have to preserve them and address them; you rarely have to restore them at the outset. PD 31B makes accessibility and retrieval cost part of the reasonableness balance, so the defensible pattern is: catalogue and preserve the snapshots, search the live sources, and restore selectively where a demonstrated need (typically suspected deletion, or gaps in live data) justifies the cost, with the analysis recorded in the DRD.

Can we rely on keywords alone?

PD 31B warns against exactly that: keyword searches alone may be inadequate, over- and under-inclusive at once. Keywords are one lever among seven, working with custodian and date scoping, analytics, review and sampling. A search description that says "we applied the agreed terms" and nothing else is describing a culling step, not a search.

Are we required to use TAR?

Not required, but in volume cases expect to explain a decision not to: the DRD asks the question, the courts have endorsed the technology since Pyrrho, and a party proposing expensive linear review of a large population will face the obvious proportionality point. The safe course is to make the decision on tested numbers and record it either way.

A relevant document has surfaced that our search never caught. Is the certificate wrong?

Not necessarily. If the search was reasonably designed, tested and honestly described, a missed document is the accepted cost of reasonableness: disclose it now, check whether it signals a system at i c gap (a channel, a term family, a custodian), fix the gap if so, and record what was done. The certificate is wrong only if it described a search that was not in fact performed, which is precisely what the paper trail in §13 protects against. Remember also that a known adverse document is disclosable regardless of any search.

Who decides if the parties cannot agree terms?

The court, at the CMC or on application, and it decides best when handed short, numbered disputes with hit data and sampling evidence attached. Parties who arrive with tested positions usually settle the list at the door; parties who arrive with adjectives get orders neither side likes. cflab. u k · e-discove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915 Page 21 of 24