

Control Of Electronic Documents What Lawyers Need To Investigate

Understanding "control" of electronic documents is crucial for UK lawyers. This guide explores the legal test, categories of documents, and investigation steps, covering subsidiaries, employees, cloud platforms, and third parties. It assists practitioners in identifying and managing relevant electronic information.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-29.

<https://e-discovery.uk/library/control-of-electronic-documents-what-lawyers-need-to-investigate>

CONTROL OF DOCUMENTS · A GUIDE FOR UK LAWYERS Control of Electronic Documents
What Lawyers Need to Investigate COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 What "control" means in plain English 03 The legal test and the leading authorities 04 Subsidiaries and parent companies 05 Employees, personal devices and personal accounts 06 Contractors and consultants 07 Outsourced providers and managed services 08 Cloud platforms: your tenancy, their servers 09 Former staff 10 True third parties, and the routes to their documents 11 The control decision tree 12 The investigation: what to gather and record 13 Cross-border complications 14 Common mistakes and technical limitations 15 Questions to ask: client, opponent, provider 16 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: WHAT DOES "CONTROL " MEAN?

§ 02 · FIRST PRINCIPLES What "control" means in plain English

§ 03 · THELAW The legal test and the leading authorities FOR THE PRACTITIONER AUTHOR
IT Y WHAT IT DECIDES, IN PRACTICE

§ 04 · THECATEGORIES Subsidiaries and parent companies

§ 05 · THECATEGORIES Employees, personal devices and personal accounts

§ 06 · THECATEGORIES Contractors and consultants

§ 07 · THECATEGORIES Outsourced providers and managed services

§ 08 · THECATEGORIES Cloud platforms: your tenancy, their servers

§ 09 · THECATEGORIES Former staff

§ 10 · THECATEGORIES True third parties, and the routes to their documents ROUTE WHEN
IT FITS

§ 11 · THE DECISION The control decision tree QUESTION1 YES/NO QUESTION2
QUESTION3 QUESTION4

§ 12 · THE INVESTIGATION The investigation: what to gather and record GATHER BECAUSE
IT ESTABLISHES

§ 13 · COMPLICATIONS Cross-border complications

§ 14 · WHERE IT GOES WRONG Common mistakes and technical limitations Common mistakes
Technical limitations

§ 15 · INTERROGATORIES Questions to ask Ask your client Ask your opponent Ask an e
Discovery / forensic provider

§ 16 · DRAFTING AIDS Suggested wording for instructions
REQUEST TO A CUSTODIAN REGARDING PERSONAL DEVICES AND ACCOUNTS (CORE PAR
AGRAPHS) PRESERVATION AND ACCESS NOTICE TO PROVIDER OR GROUP ENTITY (CORE

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

§ 18 · COMMON QUESTIONS Frequently asked questions What does "control" of electronic
documents mean? Do our parent's or subsidiary's documents count as ours? Can we really be
expected to deal with employees' personal Whats Apps? The data is in the cloud, so is it the
provider's, not ours? What if the foreign subsidiary refuses, or local law blocks transfer?
Does control end when we no longer hold the document?

§ 19 · REFERENCE Glossary BYOD Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab
Speak to a forensic examiner, not a salesperson. INSTRUCT THE LAB
NEW ENQUIRIES EMAIL - DISCOVERY

Questions and answers

What does "control" of electronic documents mean?

Under CPR 31.8 and PD 57AD, a document is within a party's control if the party has or had physical (or systems) possession of it, a right to possession, or a right to inspect or take copies. In electronic practice that reaches the client's tenancies and devices, data held by providers and agents on the client's behalf, group companies' documents where possession, rights or standing arrangements exist, and, through the structured-request mechanism, work material on custodians' personal devices and accounts. It is established by investigation (contracts, tenancy administration, actual practice), asserted in the DRD, and testable by the court.

Do our parent's or subsidiary's documents count as ours?

Not automatically: share hold in g alone is not control (Lonrho). But they do count where your client administers the relevant systems (shared tenancies decide many cases), holds contractual rights to the documents, or benefits from an arrangement in fact under which they are available on request (North Shore; Pipia). Analyse it entity by entity, and expect your opponent's group to be probed on the same basis.

Can we really be expected to deal with employees' personal Whats Apps?

Yes, where they were used for relevant work. The Court of Appeal in *Phones 4U v EE* endorsed exactly this machinery: the employer asks custodians, in agreed written terms, to make work-related material available for search under a protocol that protects private content. You are not seizing anyone's phone; you are making, and recording, a structured request, and a refusal becomes a fact the court can act on.

The data is in the cloud, so is it the provider's, not ours?

No. Data inside your client's tenancy is within your client's control: the client administers it and has contractual rights to it, and the courts treat it exactly like on-premises data. What sits outside easy reach is some provider- side material (certain logs, post-retention remnants), which is a narrower question of contract and request, and one to ask early because provider windows are short.

What if the foreign subsidiary refuses, or local law blocks transfer?

Take the steps the position allows and evidence everything: invoke the arrangements, make the request, take local advice on the restriction, propose managed alternatives (in-country processing and review, targeted extraction, transfer mechanisms), and put any genuine impediment before the English court with evidence. Courts distinguish sharply between parties who engaged with the problem and parties who deployed it.

Does control end when we no longer hold the document?

The duty catches documents that are or were in control: documents no longer held must still be identified in the disclosure exercise, with their fate stated. That is one more reason the control schedule records history (what was held, when, what happened to it) and not just the current position.

Source: <https://e-discovery.uk/library/control-of-electronic-documents-what-lawyers-need-to-investigate>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.