

Document Management Systems In Disclosure

Document management systems, such as iManage and Net Documents, record every version and interaction with a document. This guide explores their anatomy, histories, and collection methods, offering practical advice for UK litigators on leveraging DMS evidence in disclosure.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.

<https://e-discovery.uk/library/document-management-systems-in-disclosure>

DMSEVIDENCE · A GUIDE FOR UK LAWYERS Document Management Systems in Disclosure
iManage, Net Documents and the Version History That Decides Professional Disputes
COMPUTER FORENSICS LAB

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

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the drafting record as witness 03 DMS anatomy: workspaces, profiles, versions and filed email 04 Histories: versions, access logs and activity trails 05 Collection: extracting matters without flattening them 06 Privilege and third-party complications 07 Departing fee earners and DMS exfiltration 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

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT:
THEDMSKEEPSEVERYVERSIONANDLOGSEVERYTOUCH: COLLECTITSOBOTHSURVIVE

§ 02 · FIRST PRINCIPLES The problem in plain English: the drafting record as witness

§ 03 · THE SYSTEM DMS anatomy: workspaces, profiles, versions and filed email

§ 04 · THE HISTORIES Histories: versions, access logs and activity trails

§ 05 · GETTING IT OUT Collection: extracting matters without flattening them

§ 06 · WHOSE PRIVILEGE Privilege and third-party complications

§ 07 · THE LEAVING PARTNER Departing fee earners and DMS exfiltration

§ 08 · THE WIDER MAP Source architecture: where else the evidence lives EVIDENCE SYNC
CO-ADVISER DMS EMAIL BACKUPS / DELETED / (NATIVE) ESTATE ARCHIVES
RECOVERABLE DEVICE / CLIENT & CACHES COPIES

§ 09 · IN THE WILD Worked examples EXAMPLE 1 ·
THE CLAUSE THAT VANISHED BETWEEN VERSIONS EXAMPLE 2 ·
THE PARTNER WHO READ NINETY FILES IN A WEEK EXAMPLE 3 ·
THE FLATTENED PRODUCTION, UNFLATTENED

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

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask
your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED
WORDING · DMS LIMITS FOR THE PRESERVATION LETTER

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

§ 13 · COMMON QUESTIONS Frequently asked questions Is a former client entitled to the
firm's DMS versions, or only the final file? Can the DMS prove who actually made a disputed
edit? The firm migrated DMS three years ago and history "starts" there. Suspicious? What can
be proved about a fee earner who "just looked" at files before leaving? Our opponent's DMS is
cloud-hosted. Does that change anything? Are saved document comparisons really that
important?

§ 14 · 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. INSTRUCT THE LAB
NEW ENQUIRIES EMAIL - DISCOVERY

Questions and answers

Is a former client entitled to the firm's DMS versions, or only the final file?

In negligence litigation, the drafting record for the client's matters is squarely disclosable: versions, profiles and activity are documents within the firm's control bearing directly on the pleaded work: and finals-only production meets Example 3's challenge. The firm's separate post-dispute self-advice is its own privileged stream, identified and carved out rather than used to fog the matter file.

Can the DMS prove who actually made a disputed edit?

To the credential, yes: version author, check-out records and activity logs name the login and time: and the hand behind it runs the standard ladder: secretarial-save practices, shared logins and delegation established from the firm's working patterns, device artefacts where it matters. Version comments and the surrounding email round usually complete the attribution the author field starts.

The firm migrated DMS three years ago and history "starts" there. Suspicious?

Usually structural: migrations commonly carry latest versions and shed ladders: the finding is the boundary's date against the migration records, then the rebuild: pre-migration backups and archives, the attachments trail (every emailed draft is a dated version), and the client's own set. Suspicion attaches only where the boundary's timing or selectivity tracks the dispute rather than the project plan.

What can be proved about a fee earner who "just looked" at files before leaving?

Access alone proves access: the finding becomes conduct through pattern against baseline (volume, breadth beyond live matters, timing), pairing with output events (prints, exports, emails out), and the downstream chain on devices and personal accounts per guides 41 and 69: Example 2's construction. Looking is lawful; the fortnight table is what tribunals act on.

Our opponent's DMS is cloud-hosted. Does that change anything?

Route, not obligation: SaaS platforms constrain database-level acquisition, so collection runs on the platform's export and API facilities: capability audited per deployment, the version-complete and history-complete requirements unchanged, and provider retention (activity-log windows especially) making the early freeze more urgent, not less.

Are saved document comparisons really that important?

Repeatedly decisive: a saved or emailed redline is a contemporaneous statement of exactly what changed between versions, made by the parties themselves, with a date: it collapses "nobody noticed the deletion" defences (someone ran the compare) and anchors drafting chronologies without expert reconstruction. They are requested by name in every DMS matter for that reason. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915 Page 15 of 17

Source: <https://e-discovery.uk/library/document-management-systems-in-disclosure>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.