SharePoint As A Disclosure Source

SharePoint presents unique challenges and opportunities for electronic disclosure. This guide explores its architecture, including libraries, versions, permissions, and deletion, to help practitioners understand and manage this complex data source effectively in UK litigation.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/sharepoint-as-a-disclosure-source

SHARE POINT EVIDENCE · A GUIDE FOR UK LAWYERS Share Point as a Disclosure Source Libraries, Versions, Permissions and Deleted Sites: the Shared Estate and Its Collaborative Metadata COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM PERMISSION & ACCESS 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 file server that got a memory 03 Site anatomy: libraries, lists, pages and their records 04 Versions and collaborative metadata 05 Permissions, inheritance and the possibility map 06 Deletion at every scale: files, libraries, sites 07 Collection: keeping the shapes that matter 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: GUIDE43 ' STHREELAYERS, WITHBETTERRECORDSANDNEW WAYSTOLOSETHEM

§ 02 · FIRST PRINCIPLES The problem in plain English: the file server that got a memory

§ 03 · THEESTATE Site anatomy: libraries, lists, pages and their records

§ 04 · THEDRAFTINGRECORD Versions and collaborative metadata

§ 05 · WHO COULD Permissions, inheritance and the possibility map

§ 06 · GONE, ATWHATSCALE Deletion at every scale: files, libraries, sites

§ 07 · GETTINGTHESHAPESOUT Collection: keeping the shapes that matter

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE SYNCED SITE (CONTENT + TEAMS / EMAIL AUDIT + BACKUP DELETED / VERSIONS + COUNTERPARTS DIRECTORY LAYER RECOVERABLE RECYCLE) MEMBERS' DEVICES

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEINHERITANCEBREAKNOBODYDECLARED EXAMPLE2 · THEVANISHEDPROJECTSITE, THREERESTORESDEEP EXAMPLE3 · THEMIGRATIONTHATLOOKEDLIKEBACKDATING

§ 10 · WHEREITGOESWRONG 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 · SHAREPOINTLIMBFORTHECOLLECTIONSPECIFIC AT ION

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

§ 13 · COMMON QUESTIONS Frequently asked questions Do we really need version histories for every document? Can we find out who accessed a confidential folder, and when? A whole site has been deleted. What is the realistic sequence? The other side says a permission change was "routine housekeeping". How is that tested? How does Teams complicate the Share Point picture? What single export should a c company every Share Point dispute?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab 35 with windows and grains stated; through e-discovery.uk, site collections land in review structured, Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

Do we really need version histories for every document?

Not for every document: for the ones the issues touch, as series; for the rest, the latest state with the settings exhibited so truncation is known. The scoping dial (guide 37) applies: what must never happen is a drafting-or- timing dispute served with latest-states only: the platform kept the answer, and disclosure that omits it invites both the §11 request and the inference behind it.

Can we find out who accessed a confidential folder, and when?

Two layers: possibility (the computed permission map as at the dates: who could) and actuality (audit access events within their reach: who did). Both are data; neither is complete without the other; and the honest report presents them as the pair: the pool, then the recorded visits: with the audit window stated. Beyond the window, possibility plus surrounding conduct is what exists, and the report says so.

A whole site has been deleted. What is the realistic sequence?

Order of operations: the admin recycle bin (whole-site restore within the window: hours, not heroics); the deletion event from audit (account, date: the chronology regardless); tenant backup sets (guide 49's targeted restoration); members' sync mirrors (per-library echoes on devices); and the circulated-copy trail. Example 2 ran all five. The realistic answer in most estates: substantially recoverable, with the deletion's own record doing separate work.

The other side says a permission change was "routine housekeeping". How is that tested?

On its records: the change's date against the dispute's chronology; its author and their proximity to the issues; its shape (a broad tidy-up touches many objects; Example 1's break touched one folder before one panel); and its documentation (change tickets, IT practice). Housekeeping is a real phenomenon with a recognisable signature: the analysis distinguishes it from curation, and the audit stream supplies the material either way.

How does Teams complicate the Share Point picture?

Every Team is a site: channel files live in Share Point libraries auto-created per Team, private channels get their own sites, and chat-shared files route through One Drive: so the census must resolve Teams into their storage reality, and a "Teams files" request is a SharePoint/OneDrive request wearing a different name. Guide 56 takes the conversation layer; this guide's disciplines govern the files it points at.

What single export should a c company every Share Point dispute?

The permission-and-sharing state for the contested locations, with inheritance breaks and their audit history: one structured export that answers "who could", dates every deliberate change to the audience, and either dissolves or establishes the case's access theory before witness statements calcify. It is cheap, it is data, and Examples 1 and 3 between them show both directions it cuts. cflab. u k · e-disc ove r y. u k