



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

SharePoint as a Disclosure Source

Libraries, Versions, Permissions and Deleted Sites: the Shared Estate and Its Collaborative Metadata

SharePoint is the corporate file server's successor and inheritor of all its disputes: who could see the folder, who changed the document, where the library went: now with richer records than the file server ever kept. Sites and libraries carry per-document version series with named authors, permission structures queryable as data, sharing histories, and a recycle system that catches deletions at two stages: while site deletions, permission inheritance, and the migration history from the old file server add traps of their own. This guide treats SharePoint as guide 43's file server evolved: the three layers of content, history and context; collection that keeps the collaborative metadata; the possibility-map discipline for shared spaces; and the deleted-site and reorganisation scenarios where whole evidential estates seem to vanish and rarely have.

© Estimated reading time: 26 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. SharePoint estates run through its commercial casework as the file server once did: library collection with versions and permissions, deleted-site recovery, access-dispute analysis, and the migration archaeology that explains why "the 2019 folder" looks the way it does. Its eDiscovery arm, **e-discovery.uk**, processes site collections at disclosure scale.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

SHAREPOINT & SITE COLLECTION

PERMISSION & ACCESS ANALYSIS

CPR PART 35 EXPERT REPORTS

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

Executive summary

THE HEADLINE POINT: GUIDE 43'S THREE LAYERS, WITH BETTER RECORDS AND NEW WAYS TO LOSE THEM

SharePoint is the shared documentary estate, and everything guide 43 taught about file servers transfers with upgrades. **Content:** libraries of documents with platform-maintained metadata: created/modified with modifying accounts, and per-document version series (named, timestamped saves: the drafting history guide 50 differencing runs on) kept by default. **History:** the version series themselves, the two-stage recycle system (user then site-collection bins, roughly 93 days combined), deleted-site retention (removed sites recoverable by admins for a bounded period), and beneath everything the tenant's backup layer. **Context:** permission structures as queryable data: site, library, folder and item-level grants, inheritance and its breakages, sharing links: plus the audit stream (guide 57) recording access, edits, downloads, sharing and deletion as events. The new hazards are structural: **permission inheritance** means one careless site-level grant exposes everything beneath it, and a broken-inheritance folder hides an exception nobody remembers making: the possibility map must be walked, not assumed; **reorganisations and migrations** (file-server-to-SharePoint, site restructures, Teams-driven site sprawl) rewrite paths and dates in ways that mimic tampering to the unwary (guide 43's migration-literacy point, redoubled); and **site-scale deletion:** a whole estate removed in one admin action: has its own recycle window and audit trail, making "the site is gone" a bounded, checkable claim rather than a catastrophe. Collection keeps the shapes: structure, versions, permissions and sharing as data, by the guide 52 route the matter warrants: because SharePoint's evidential riches are mostly relational, and flat exports throw them away.

- **Version series are the platform's gift:** named per-save histories on by default across the estate: collect them, difference them, and refuse last-touch attribution (guide 54's Example 3, at estate scale).
- **The possibility map is data here:** permissions and inheritance are exportable and analysable: "who could access X on date D" is a query, then a finding: run it before anyone pleads exclusivity.
- **Deleted sites have a recycle bin too:** admin-recoverable within the window: the first check when an estate "disappears", before anyone reaches for backups.
- **Migration dates are not action dates:** bulk-rewritten timestamps from the file-server move or a restructure are read with the migration history open: the false-tampering trap, avoided.
- **Holds and week-one apply estate-wide:** site preservation, recycle suspension in effect via holds, audit export: guide 51's playbook names the sites, not just the custodians.

The problem in plain English: the file server that got a memory

The old file server (guide 43) forced examiners to reconstruct history from snapshots and infer possibility from permission exports taken today. SharePoint keeps the history itself: every save a version with a name on it, every share an event, every permission change in the audit stream: which transforms what disclosure can prove, and raises the standard for what parties should be asked to produce. A dispute about a document's evolution, a folder's audience or a deletion's timing is no longer inferential: the records exist, and the only questions are whether they were preserved (week one), collected with their shapes intact (this guide's §7), and read competently (the possibility map, the migration history, the version series).

The corresponding failure mode is producing SharePoint as if it were a file share: current documents, flat, no versions, no permissions, no sharing states: disclosure that is technically responsive and evidentially gutted. The requests in §11 exist to stop opponents doing that to you, and the specification in §7 to stop your own side doing it to itself.

Site anatomy: libraries, lists, pages and their records

- **Sites and their sprawl:** the estate is sites: departmental, project, and the auto-created site behind every Team and group (guide 56's overlap): the site inventory, with owners and creation dates, is the scoping census, and Teams-era sprawl means it is always longer than the client thinks.
- **Document libraries:** the folders-and-files layer, with per-item metadata, versions and permissions: the disclosure workhorse, collected structurally.
- **Lists:** structured data (registers, trackers, custom applications) with item-level version histories of their own: frequently the operational record (the complaints register, the approvals tracker) that decides regulatory and process disputes, and frequently forgotten because it is not "documents".
- **Pages and news:** the intranet layer: announcements, policies as published, with their own versioning: what the organisation told itself, dated: the constructive-knowledge exhibit.
- **Site-level records:** membership and ownership, storage metrics, external-sharing configuration: the context layer's site-scale entries, exported as exhibits per estate.

Versions and collaborative metadata

- **Per-save series, named:** each version carries author account and timestamp: the estate-wide drafting history, subject to version limits and trimming (both detectable: limits in settings, trimming in audit).
- **Co-authoring's grain:** simultaneous editing interleaves contributors within versions: guide 50's caution governs sentence-level claims; the platform's finer activity records and the report's honest grain-setting do the rest.
- **Check-out, approval and workflow records:** libraries running check-out or approval keep those events per version: the formal-process paper trail (who approved the policy, when) that governance disputes turn on.
- **Item metadata columns:** business-configured columns (status, owner, matter number) with their own change history via versions: the operational context reviewers need and flat exports lose.
- **Differencing at estate scale:** guide 50's method across libraries: the disputed agreement's series, the policy's evolution, the register's edit history: the deliverable remains the dated timeline with authors where the platform names them.

Permissions, inheritance and the possibility map

- **Inheritance as the default story:** permissions flow site → library → folder → item unless broken; the map is therefore read top-down, with every inheritance break enumerated: each break is a decision someone made, dated in audit, and often the finding itself.
- **Groups within groups:** grants resolve through M365 groups and security groups: the effective audience of a folder is computed, not read off: the analysis "who could access X on date D" resolves memberships as at that date from directory records.
- **Sharing links overlay everything:** item-level links (people-specific, org-wide, anyone) widen audiences past the permission structure: collected as states plus audit events, per guide 54's discipline.
- **External sharing configuration:** per-site external policies define whether outsiders could ever be in the audience: the one-line export that reframes leak inquiries.
- **The exclusivity discipline:** "only she could access it" is pleaded after the computed map says so, and not before: guide 43's Example 3, with better data and less excuse.

Deletion at every scale: files, libraries, sites

- **Files and folders:** the two-stage recycle march with dates and deleting accounts: guide 54's walk, on shared ground where the deleting account matters more.
- **Libraries and lists:** deletable as units into the same recycle system: a vanished register is usually one restore away within the window.
- **Sites:** deleted sites sit in the admin recycle bin for a bounded period (around 93 days), restorable whole: the first check when an estate disappears: with the deletion event (account, date) in audit regardless of recovery.
- **Retention policies as quiet deleters:** policy-driven disposal runs on schedules parties forget: the policy inventory explains gaps innocently, or fails to: either way it is exhibit one in any missing-content dispute.
- **After the windows:** holds preserved what they covered; the tenant backup layer and the architecture paths (§8) carry the rest: and the audit stream's deletion events remain the chronology even where content is gone.

Collection: keeping the shapes that matter

- **Structure preserved:** site/library/folder paths intact in the collection and its manifests: provenance reviewers and courts can follow.
- **Versions as series:** where the issues touch drafting or timing, version histories collected as data (the API route's home ground, per guide 52's structural case): not just latest states.
- **Permissions and sharing as data:** the possibility map's inputs: permission reports, inheritance breaks, link inventories: collected as at now and reconstructed as at the relevant dates from audit.
- **Lists as lists:** structured exports keeping columns and item histories: the register collected as the register, not as ten thousand printouts.
- **Scope by site census:** the inventory from §3 drives proportionate scoping (guide 37's dial): named sites and libraries, with Teams-connected sites resolved so nothing in scope hides behind a product name.

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine the site in isolation. SharePoint content coexists in: synced copies on members' devices (library sync spreads guide 54's mirrors across every participant); OneDrive origins (documents moved or shared from personal drives, with their own version prehistory); Teams (the same files surfaced in channels, plus the conversation about them: guide 56); email (attachments as sent: the counterpart trail of every circulated draft); the audit and directory layers (events, memberships-as-at-dates); third-party tenant backups (site states across months); the old file server and its migration artefacts (the pre-history, per guide 43); and recipients' estates where external sharing ran. When the site's own layers have expired or the site is gone: members' sync mirrors, the backup layer and the circulated-copy trail reconstruct the estate, and the audit export frames what stood where.

EVIDENCE	SITE (CONTENT + VERSIONS + RECYCLE)	MEMBERS' SYNCED DEVICES	TEAMS / EMAIL COUNTERPARTS	AUDIT + DIRECTORY	BACKUP LAYER	DELETED / RECOVERABLE
Documents	Y, structurally	Mirrors per member	As-shared / as-sent copies	Access + edit events	Y where deployed	Two-stage recycle; site bin
Drafting history	Y: version series	Local shadow layers	Circulated generations	Edit events	Generational states	Trimming detectable in audit
Who could access (date D)	Permission data now	n/a	Membership context	Y: computed as-at	Point-in-time states	Reconstructable
Deletion chronology	Recycle metadata	Mirror divergence	n/a	Y: events with accounts	Bracketing sets	Events outlive content
Vanished sites	Admin recycle bin (window)	Members' mirrors: the estate's echo	Linked-file remnants	Deletion event: Y	Y: whole-site states	Window, then backup layer

Fallback strategy in one line: a vanished library or site is checked in order: admin recycle bin, members' sync mirrors, backup sets, circulated copies: with the audit deletion event anchoring the chronology whichever path restores the content.

Worked examples

EXAMPLE 1 · THE INHERITANCE BREAK NOBODY DECLARED

A discrimination claimant alleged she had been excluded from the promotion-panel materials her comparators could see. The respondent asserted uniform access: "the HR site permissions applied to everyone at her grade". The map said otherwise: the panel folder carried a broken inheritance, created (audit event, the HR director's account) eleven days before the panel sat, replacing site permissions with a named list: her comparators present, her name absent. The break's date, author and membership were data, not testimony; the respondent's uniform-access evidence was withdrawn, and the folder's little exception became the tribunal's central chronology entry.

EXAMPLE 2 · THE VANISHED PROJECT SITE, THREE RESTORES DEEP

A JV dispute's key estate: the joint project site: was "decommissioned in a tidy-up" a month before proceedings, past the admin recycle window by the time lawyers engaged. Three paths rebuilt it: the tenant's third-party backup held monthly site states across the project's life (restored per guide 49); four team members' laptops carried synced mirrors of the main library, one disconnected early enough to predate a contested deletion; and the circulated-copy trail: every board pack emailed out: supplied as-sent generations from counterpart mailboxes. The deletion event itself (account, date, three weeks after the letter before action) ran through the spoliation argument, while the reconstructed estate ran through the merits. The site had gone; the ensemble had not, and the tidy-up's timing cost more than the tidying saved.

EXAMPLE 3 · THE MIGRATION THAT LOOKED LIKE BACKDATING

A claimant's expert reported that a critical policy document's created date post-dated the events it governed: fabrication, the claim went, of a policy after the fact. The respondent's examination read the estate's history instead of one field: the site had received the file-server migration eighteen months earlier, created dates rewritten en masse (the migration batch's signature across thousands of files, per guide 43's literacy point); the document's version series began at migration with content already mature; and the pre-history: the file server's backup sets: held the policy two years earlier, hash-continuous with version 1. The backdating allegation had been a migration artefact read by someone who examined a metadata field and not an estate. It was withdrawn, with the respondent's costs of the exercise.

Common mistakes and technical limitations

Common mistakes

- **Flat production:** current documents without versions, permissions or structure: the gutted disclosure §2 warns of.
- **The site census skipped:** Teams-created sites and legacy estates outside a scope drawn from the org chart.
- **Exclusivity pleaded off today's permissions:** the as-at-date computation never run; Example 1's inverse.
- **Migration-date findings:** Example 3's allegation: created dates read without the migration history.
- **Lists forgotten:** the operational registers absent because scoping asked only for "documents".
- **Vanished sites mourned, not checked:** the admin recycle bin and members' mirrors unvisited.
- **Retention policies undiscovered:** gaps litigated as concealment that a disposal schedule explains: or gaps explained by a schedule nobody verifies.
- **Version trimming unread:** single-version disputed documents accepted at face value (guide 50's flag, estate edition).

Technical limitations

- **Windows bound the recycle layers:** the marches expire; holds and backups extend; the report states which applied.
- **As-at permission reconstruction depends on audit reach:** beyond the log's window, the map is partial and says so.
- **Co-authoring grain persists:** version authorship is save-level; finer claims need finer records.
- **Version limits truncate silently:** long-lived documents may have lost early series to configured caps: settings exhibited, truncation stated.
- **Estate sprawl is real:** completeness claims are made per census, not per assumption: "all relevant sites" means the inventory was walked.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- The site census: which sites touch the issues, including Teams-connected and legacy estates: with owners and the migration history?
- What retention and disposal policies run on those sites, and what has the schedule deleted in [period]?
- For the key documents: are version series intact, and what do the settings cap them at?

Ask your opponent

- Please preserve the sites at [list], including version histories, both recycle stages, permission and sharing states, and suspend all retention-driven disposal; confirm hold coverage and dates.
- Please produce, for [folder/document], the version series with authors and timestamps, the permission structure including inheritance breaks with their audit history, and sharing links with creation and access events.
- If any site, library or list relevant to the issues has been deleted or restructured since [date], please give particulars: what, when, by whom, and what recovery paths remain.

Ask your eDiscovery / forensic provider

- What does the census-driven scope look like, and which sources need structural (API) collection?
- Can you compute the possibility map as at the relevant dates: and what does audit reach permit?
- For the timestamp disputes: what does the migration and version history actually support?

SUGGESTED WORDING · SHAREPOINT LIMB FOR THE COLLECTION SPECIFICATION

"For the sites at Schedule A: (a) collection shall preserve site, library and folder structure, and shall include document version histories as series with authorship and timestamps, list contents with item version histories, and page libraries where in scope; (b) permission structures (including inheritance breaks and group resolutions), sharing links and external-sharing configuration shall be collected as structured data, as at collection and, from audit records, as at the dates at Schedule B; (c) both recycle stages and, where applicable, the site-collection recycle bin shall be enumerated with deletion metadata; and (d) the report shall state hold coverage, retention policies in force, version-limit settings and migration events material to timestamp interpretation."

Checklist and red flags · When to involve a digital forensic expert

The SharePoint checklist

- ☐ Site census run: departmental, project, Teams-connected, legacy: with owners and dates
- ☐ Holds and preservation cover the named sites; retention disposal suspended; week-one audit export taken
- ☐ Collection structural: paths, versions-as-series, permissions-as-data, lists-as-lists
- ☐ Possibility map computed as at the relevant dates; inheritance breaks enumerated with audit history
- ☐ Migration history obtained before any timestamp is argued
- ☐ Recycle stages and the site bin enumerated in every deletion dispute
- ☐ Version settings and trimming checked on the disputed documents
- ☐ Vanished estates walked through the fallback order before loss is conceded
- ☐ Retention policies exhibited wherever gaps are in issue
- ☐ Members' sync mirrors in the device plan for contested libraries

Red flags

- Production of current files only from a versioned estate.
- An inheritance break created near a key date.
- A site deleted after the duty arose, "in a tidy-up".
- Created dates argued from a migrated estate without the batch history.
- A register (list) missing from disclosure that the business plainly ran on.
- Exclusivity claims with no as-at computation attached.
- Disposal schedules that accelerated during the relevant period.

When to involve a digital forensic expert

At the census and specification, so scope and structure survive review; at the possibility map, where computed as-at answers replace assertions (Example 1's engine); at every timestamp dispute on a migrated estate, before allegations are made or met (Example 3's rescue); and at vanished-estate reconstruction, where the fallback order and the guide 49 restoration run together (Example 2). Reported under CPR Part 35 with windows, grains and audit reach stated: and through **e-discovery.uk**, site collections processed so structure and versions inform review instead of drowning it.

§ 13 · COMMON QUESTIONS

Frequently asked questions

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 SharePoint picture?

Every Team is a site: channel files live in SharePoint libraries auto-created per Team, private channels get their own sites, and chat-shared files route through OneDrive: 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 accompany every SharePoint 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.

§ 1 4 · REFERENCE

Glossary

Admin recycle bin

The site-scale bin holding deleted sites for a bounded window.

As-at computation

The possibility map resolved for a past date from audit and directory records.

Census (site)

The estate inventory: departmental, project, Teams-connected, legacy.

Inheritance break

A location's departure from inherited permissions; a dated decision.

Library sync

Members mirroring shared libraries locally; the estate's device echoes.

List

Structured data with item version histories; the operational register layer.

Migration batch signature

Mass-rewritten dates marking an estate move; timestamp context.

Possibility map

The computed audience of a location; guide 43's discipline as data.

Site-collection recycle

Stage two of the file-level march.

Version limit

The configured cap truncating old series; exhibited, not assumed.

Sources and authoritative references

The estate disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (SharePoint collection, permission and access analysis, deleted-site recovery, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation, Phase 03 · Collection and Phase 04 · Processing (structural site collection into review): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection · e-discovery.uk/edrm/processing
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Microsoft documentation: SharePoint retention and deletion: learn.microsoft.com, [retention and deletion](https://learn.microsoft.com) · learn.microsoft.com, Purview eDiscovery
- PD 57AD and CPR Part 35: justice.gov.uk, [PD 57AD](https://justice.gov.uk) · justice.gov.uk, [Part 35](https://justice.gov.uk)
- ICO, UK GDPR guidance: ico.org.uk

DISCLAIMER

This publication provides general information about SharePoint evidence as at August 2026. Platform behaviour, windows and defaults change on Microsoft's schedule and vary by tenant and configuration; verify current behaviour in the matter at hand. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

SharePoint estates are collected and read at the laboratory with the shapes intact: census-driven scoping; structural collection (versions as series, permissions and sharing as data, lists as lists) by the route guide 52 selects; possibility maps computed as at the dates that matter; migration histories read before timestamps are argued; and vanished estates walked through the fallback order: admin bin, mirrors, backups, circulated copies: with the deletion events anchoring chronology throughout. Examples 1-3 are the practice's standing shapes: the dated inheritance break, the three-path site reconstruction, the migration artefact defused. Reporting is CPR Part 35 with windows and grains stated; through **e-discovery.uk**, site collections land in review structured, deduplicated and readable. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; if a site or schedule is deleting while positions are drafted, the suspension call comes first.



I N S T R U C T T H E L A B

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES

+44 (0)20 7164 6971

EMAIL

info@cflab.uk

E-DISCOVERY

e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom

cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace