

# Should Backup Systems Be Searched For Disclosure

This guide explores the complex issue of searching backup systems for electronic disclosure in UK litigation. It addresses preservation, proportionality, and the decision framework for when such searches are necessary, particularly when backups hold the sole remaining evidence. Practical advice on targeted restoration and arguing the point is included.

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

<https://e-discovery.uk/library/should-backup-systems-be-searched-for-disclosure>

BACKUP S IN DISCLOSURE · A GUIDE FOR UK LAWYERS Should Backup Systems Be Searched for Disclosure? Preservation, Proportionality and the Cases Where the Backup Is the Only Copy Left COMPUTER FORENSICS LAB

## § ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the archive every one hopes to ignore 03 Preserve first, argue later: the legal baseline 04 Know what you actually have: backup technology in 05 When backups should be searched: the decision framework 06 Doing it well: targeted restoration methodology 07 Arguing the point: for access, and against it 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: PRESERVATION IS NEAR - AUTOMATIC; SEARCH IN COURT IS A REASONED, EVIDENCED CHOICE

§ 02 · FIRST PRINCIPLES The problem in plain English: the archive everyone hopes to ignore

§ 03 · THE BASELINE Preserve first, argue later: the legal baseline

§ 04 · KNOW YOUR STATE Know what you actually have: backup technology in GENERATION WHAT IT LOOKS LIKE, AND WHAT RESTORATION REALLY COSTS

§ 05 · THE DECISION When backups should be searched: the decision framework

§ 06 · DOING IT WELL Doing it well: targeted restoration methodology

§ 07 · THE ARGUMENT Arguing the point: for access, and against it

§ 08 · THE WIDER MAP Source architecture: where else the evidence lives EVIDENCE + LIVE SYSTEM RECYCLE LAYERS SNAPSHOTS / BACKUP ARCHIVE / COUNTERPART DELETED / REPLICAS GENERATIONS JOURNALING COPIES RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 ·  
THELEAVERPROCESSANDTHEQUARTER - ENDTAPES EXAMPLE2 ·  
THEHOLDTHATNEVERREACHEDTHEROTATION EXAMPLE3 · THE " RUINOUS "  
RESTORATIONREPRICED

§ 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 · B AC KUPLIMBFORTHE DAY- ONEPRESER VAT IONNOTICE

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The  
backups-in-disclosure checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Do we have to preserve every  
backup we hold, forever? Are backups "disclosable documents"? Our key custodian's mailbox  
was deleted before the dispute. Is that spoliation? How much does targeted restoration actually  
cost now? Can we get access to the other side's backups directly? Cloud services back  
everything up anyway, don't they?

§ 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. INSTRUCTTHELAB  
NEWENQUIRIESEMAILE - DISCOVERY

## Questions and answers

### **Do we have to preserve every backup we hold, forever?**

No: the duty is bounded by relevance and reasonableness: suspend recycling for the systems and periods the issues touch, hold the generations that bracket the key dates, and document the bounds you chose and why. An unbounded freeze is neither required nor wise; a reasoned, notified, recorded suspension is the standard the court will actually test you against.

### **Are backups "disclosable documents"?**

The material on them is: backup copies of documents within your control are within your control, and the DRD expects them described. Whether they must be searched is the separate proportionality question this guide frames: and describing them accurately while declining to search, with reasons, is a legitimate and commonly correct position. Silence about them is neither.

### **Our key custodian's mailbox was deleted before the dispute. Is that spoliation?**

Routine deletion before any preservation duty arose is not spoliation: leaver processes are lawful housekeeping. The consequences are practical: the backup and archive layers become the custodian's only remains, the catalogue question becomes urgent (retention there is also finite), and if generations exist, the only-remaining- source test points firmly at restoration. Deletion after the duty arose is a different conversation, and Example 2 shows where it goes.

### **How much does targeted restoration actually cost now?**

On modern platforms: typically laboratory days, not months: a mailbox or file-set from catalogued disk-based sets is hours-to-days including processing; a handful of generations for evolution questions, low single-digit days. Managed tape multiplies handling but stays estimable. The open-ended numbers belong to legacy and orphaned media, where honest assessment (sample reads, environment reconstruction scoping) is the product. Any figure offered without naming the platform tier is a guess wearing a suit.

### **Can we get access to the other side's backups directly?**

Orders for restoration and disclosure of the results are the norm; direct access to an opponent's backup environment is rare and reserved for guide-32-style d is trust scenarios, usually via an independent examiner under protocol rather than party access. The productive route is almost always: catalogue disclosure, targeted restoration by them (or an agreed neutral), and the output into ordinary disclosure: sought with the engineering specificity that Example 3's reframed request modelled.

### **Cloud services back everything up anyway, don't they?**

Partially and differently: SaaS platforms run retention, recycle and version layers (excellent short-to-medium reach, per the cloud guides ahead) and providers keep their own resilience copies you generally cannot reach; many tenants add third-party backup products that behave like this guide's modern tier. The practical rule transfers intact: map the layers, read the retention windows, suspend what your side controls, and ask the catalogue question of what ever backup product the tenant runs: "it's in the cloud" is the beginning of the analysis, not its answer. cflab. u k · e-disc ove r y. u k ©2026 Computer Forensics Lab Ltd ·cflab.uk

Source: <https://e-discovery.uk/library/should-backup-systems-be-searched-for-disclosure>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.