Microsoft Purview Or Independent Forensic Collection

This guide helps UK lawyers choose the correct collection route for Microsoft 365 evidence, weighing the benefits of Microsoft Purview against independent forensic collection. It provides a decision framework, discusses hybrid approaches, and explains how to defend the chosen method in court. Common mistakes and technical limitations are also covered.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/microsoft-purview-or-independent-forensic-collection

PURVIEWVSINDEPENDENTCOLLECTION · A GUIDE FOR UK LAWYERS Microsoft Purview or Independent Forensic Collection? Choosing the Right Collection Route for a Microsoft 365 Matter: and Defending the Choice Afterwards COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM INDEPENDENT / COURT-APPOINTED EXAM IN AT I ON 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 fork every M365 matter reaches 03 What Purview does well: and where it bites 04 What independent collection adds: and what it costs 05 The decision framework: trust, structures, downstream 06 Hybrid patterns that dominate real practice 07 Defending the choice: the record that survives the CMC 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: PURVIEWFORSCOPE, INDEPENDENCEFORTRUST, HYBRIDSFOR MOSTREALMATTERS

§ 02 · FIRST PRINCIPLES The problem in plain English: the fork every M365 matter reaches

§ 03 · THEHOUSETOOLS What Purview does well: and where it bites

§ 04 · THEOUTSIDEEXAMINER What independent collection adds: and what it costs

§ 05 · THEDECISION The decision framework: trust, structures, downstream

§ 06 · HOWITACTUALLYGOES Hybrid patterns that dominate real practice

§ 07 · THE PAPER Defending the choice: the record that survives the CMC

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE PARTY PURVIEW INDEPENDENT / END POINT COUNTERPART DELETED / ROUTE API ROUTE FORENSICS TENANTS RECOVERABLE THIRD- BACKUP

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THESELF - COLLECTIONTHATCOULDNOTCARRYTHEWEIGHT EXAMPLE2 ·

THESTRUCTURESPURVIEWFLATTENED EXAMPLE3 · THECOUNTERSIGNEDMANIFEST

§ 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 · PROTOCOLCLAUSEONCOLLECTIONROUTE (A DA PT)

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

§ 13 · COMMON QUESTIONS Frequently asked questions Is Purview collection "forensic"? Will the court order independent collection if we ask? Can the two routes disagree about what exists? We already exported everything to PSTs last year. Do we start over? Does the choice differ for regulatory investigations or criminal matters? What single sentence should go in every M365 protocol?

§ 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

Is Purview collection "forensic"?

It is defensible when managed: scoped, logged, exported deliberately, manifested: and courts accept it routinely for ordinary disclosure. What it is not is independent of the tenant's operators or faithful to every structure: the two properties the word "forensic" is usually reaching for when the question gets asked. Match the label to the need: most matters need defensible; contested ones need independent or structural too, and that is a route decision, not a tooling insult.

Will the court order independent collection if we ask?

Where you can show the o per at or problem (conflicted admins, self-collection by implicated teams) or demonstrated defects (Example 1's answers, export irregularities), yes: targeted orders for independent re- collection or examiner-supervised exercises are familiar territory. A bare preference for d is trust without grounds fares poorly against proportionality. Build the application the way §7 builds the defence: on the record of who did what, not on adjectives.

Can the two routes disagree about what exists?

They can differ at the edges: index-bound search versus direct enumeration, export renderings versus structural collection: which is precisely what verification sampling exists to surface and explain. Genuine content d is agreement (an item one route finds and the other cannot) is rare and always informative: it points at index edges, timing, or conduct: and resolving it is exactly the examiner's job. The manifests make the comparison possible; run without them, d is agreement is just fog.

We already exported everything to PSTs last year. Do we start over?

Not necessarily: assess before re-collecting. The questions: what the export captured and lost (settings, metadata report, manifest: if none exist, that is the first finding), whether the matter's issues touch what was lost, and whether the tenant still holds the sources for a better pass (holds and windows, per guide 51). Sometimes the old export serves with a supplementary structural collection; some time s it is Example 1's do-over. An afternoon's expert assessment prices it before positions harden.

Does the choice differ for regulatory investigations or criminal matters?

The framework holds; the weights shift. Downstream scrutiny (question 3) is at its maximum: methods face expert challenge under CrimPR 19 or a regulator's own technical team: and o per at or independence is often effectively mandatory where the organisation's conduct is the subject. Expect independent or examiner-verified patterns as the norm, fuller method statements, and: in criminal work: the Forensic Science Regulator Code's declarations sitting over the exercise. The fork is the same; the tolerances are tighter.

What single sentence should go in every M365 protocol?

Name the o per at or and log the access: "All collection operations shall be performed by [named persons/ examiner] under scoped, time-bounded roles, with all tenant operations during the exercise logged and the logs preserved and disclosable." It costs nothing, it

disciplines both sides, and it converts the commonest category of route dispute: who touched what, when: from allegation into lookup. Most of this guide is that sentence, expanded. 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