Investigating Suspected Employee Data Theft

This guide outlines the critical steps for UK litigators, in-house counsel, and investigators dealing with suspected employee data theft. It covers lawful investigation, evidence collection, and legal deployment, emphasising preservation and speed.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
https://e-discovery.uk/library/investigating-suspected-employee-data-theft

EMPLOYEEDATATHEFT · A GUIDE FOR UK LAWYERS Investigating Suspected Employee Data Theft From First Suspicion to Springboard Relief: The Forensic Investigation Done Right COMPUTER FORENSICS LAB

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

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: exits leave trails, and panic destroys them 03 First response: triggers, containment and what not to touch 04 The exfiltration-artefact map: USB, cloud, email, print and beyond 05 Lawful investigation: UK GDPR, monitoring rules and employment process 06 Attribution, quantification and the choreography timeline 07 Legal deployment: undertakings, delivery-up and springboard relief 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: PRESERVEFIRST, INVESTIGATELAWFULLY, BUILDTHE CHOREOGRAPHY, ANDMOVEFAST: DATA - THEFTCASESAREWONBYTHEQUALITYOF THEFIRSTFORTNIGHT ' SFORENSICSANDLOSTBYTHEITDEPARTMENT ' SFIRST AFTER NO ON

§ 02 · FIRST PRINCIPLES The problem in plain English: exits leave trails, and panic destroys them

§ 03 · THE FIRST RESPONSE First response: triggers, containment and what not to touch

§ 04 · THETRAIL The exfiltration-artefact map: USB, cloud, email, print and beyond

§ 05 · INSIDETHELAW Lawful investigation: UK GDPR, monitoring rules and employment process

§ 06 · THECASEASSEMBLED Attribution, quantification and the choreography timeline

§ 07 · INTO COURT Legal deployment: undertakings, delivery-up and springboard relief

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE SYSTEM ESTATES (

§ 7 END POINT PLATFORM NETWORK / PHYSICAL IMAGE AUDIT LOGS PROXY LAYER MAIL- COUNTERPART RECORDS ROUTES)

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THESUNDAYHARVESTANDTHEMONDAYRESIGNATION EXAMPLE2 · THELOOK - AROUNDTHATNEARLYLOSTTHECASE EXAMPLE3 · THEARTEFACTSTHATTOLDANINNOCENTSTORY

§ 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 (the former employee / new employer) Ask your e Discovery / forensic provider LETTER)

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

§ 13 · COMMON QUESTIONS Frequently asked questions We suspect a departing employee right now. What are the first three actions? Can we search a leaver's work email and files without their consent? The employee used their personal Dropbox and phone. Can we get at those? What is springboard relief and why the urgency? Our IT team already went through the laptop. Is the case dead? What if the artefacts have an innocent explanation?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab 35 reports produced on injunction timetables and independent-examiner structures offered where personal Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

We suspect a departing employee right now. What are the first three actions?

Sequester their devices unpowered, place their accounts on hold rather than deletion, and export the platform audit logs: §3's freeze, all achievable today: then instruct before anyone investigates by hand. The order matters because every layer has a clock: retention on the logs, reissue on the devices, and curiosity on the rest.

Can we search a leaver's work email and files without their consent?

Generally yes for work systems under a lawful, proportionate, documented investigation: §5's UK GDPR frame: with private material encountered on those systems handled by filter in g protocol rather than free browsing. What loses cases is not exam in in g work systems; it is disproportionate trawling and undocumented purpose: the frame is the protection.

The employee used their personal Dropbox and phone. Can we get at those?

Through process: undertakings sought by letter, then delivery-up and imaging orders, commonly via an independent examiner who reports on relevant material only (§7): the personal estate is reachable, on legal timelines, and the employer-side artefacts (sync databases, upload logs) usually prove the transfer without it. Plan the route early; do not self-help into private accounts.

What is springboard relief and why the urgency?

An injunction neutralising the unfair head start taken material confers: restraining its use (and some time s competitive activity) for the period the advantage would last: which is precisely why it dies of delay: courts protect head starts still capable of neutralisation. The forensic fortnight feeds the application; a forensic quarter feeds a damages claim instead.

Our IT team already went through the laptop. Is the case dead?

Damaged, not dead: Example 2's rescue is the standard pattern: the platform, mail, network and physical layers (§8) carry their own copies of the story, and preserved backups often hold what the end point lost: an examiner maps what survives and states the contamination honestly. But stop further handling now: each additional touch narrows the rescue.

What if the artefacts have an innocent explanation?

Then finding it early is the win, which ever side you are: Example 3's dismissed application was expensive for the employer who never ran the §6 pass, and vindicating for the respondent who did: baselines (sanctioned devices, closure procedures, role-consistent access) decide what artefacts mean. The examiner's job is the supportable story; the advocate's job starts after. cflab. u k · e-disc ove r y. u k