The First EDisclosure Meeting 50 Questions Lawyers Should Ask

The first e-disclosure meeting is crucial for UK lawyers to understand a client's data landscape. This guide provides 50 questions across key areas like IT systems, data custodians, and preservation actions, helping to convert answers into practical steps for electronic disclosure.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-29.
https://e-discovery.uk/library/the-first-edisclosure-meeting-50-questions-lawyers-should-ask

THE FIRST MEETING · A GUIDE FOR UK LAWYERS The First e Disclosure Meeting 50 Questions Lawyers Should Ask COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: WHYFIFTYSTRUCTUREDQUESTIONS

§ 02 · FIRST PRINCIPLES Why the first meeting matters, practically and legally

§ 03 · METHOD How to run the meeting

§ 04 · QUESTIONS1 - IT architecture 1 · Walk me through where the organisation's data lives: email platform, file storage, chat and collaboration tools, business systems, and anything else with company information in it. 2 · Who administers those systems, and are any managed by an outside IT provider? Who holds global administrator rights? 3 · Is there a systems inventory, asset register or data map, however in form a l? Can we have it? 4 · What has changed in the estate over the relevant period: migrations, new platforms, decommissioned systems, mergers or rebrands with old domains? 5 · Which business systems record the transactions or events this dispute is about (CRM, ERP, finance, quality, sector systems), and who understands each one?

§ 05 · QUESTIONS6 - 1 Custodians 6 · Who was actually involved in the events behind this dispute: who negotiated, decided, approved, performed and recorded? Not the org chart; the people who did the work. mailbox or manage their diary? here, and on what timetable? project channel)? Who has access to each?

§ 06 · QUESTIONS11 - 1 Devices too? months before)? 15 · Do people use removable media (USB drives, external disks) or connect personal storage to work machines?

§ 07 · QUESTIONS16 - 2 Cloud services project tools, sector applications, anything paid by subscription? 17 · Do staff use personal cloud accounts (personal Gmail, Dropbox, iCloud) for anything work-related, officially or not? 18 · What messaging apps are used for business: Whats App, Signal, Telegram, i Message? By whom, with whom, and are disappearing-message settings on any where? controls and export capability? 20 · Who are the cloud accounts actually registered to? Any business accounts on a founder's or employee's personal email, or a personal number running Whats App Business?

§ 08 · QUESTIONS21 - 2 Deleted data 21 · Has anyone deleted, cleaned up, exported or reorganised anything potentially relevant since this dispute arose, or in anticipation of it? This is a safety question, not an accusation. 22 · Has anyone already investigated internally: IT looking through a laptop, HR review in g a mailbox, a manager checking a leaver's files? items folders, retention holds? you think so? involve here?

§ 09 · QUESTIONS26 - 3 Retention and backups 26 · What retention and auto-deletion policies are configured right now on email, chat and drives: the actual settings, not the policy document? (tapes, old systems) needing special handling? 30 · Have retention settings, hold policies or backup schedules been changed by anyone since the dispute arose?

§ 10 · QUESTIONS31 - 3 Preservation actions a c knowledge on behalf of IT operations? 34 · Is anything volatile enough that it should be forensic all y preserved this week: suspect devices, key handsets, CCTV, a leaver's laptop? c on firm at i on that preservation steps have been taken?

§ 11 · QUESTIONS36 - 4 Privacy and data protection 36 · What personal data will the exercise inevitably touch: employees' communications, customers' information, special-category data in HR or health contexts? 37 · What do staff-facing policies say about monitoring and the company's access to work communications, and what have staff actually been told? 38 · Where personal devices hold work material, are the individuals likely to cooperate with a targeted, privacyprotective extraction? Any relationships already strained? 39 · Is any relevant data outside the UK: foreign subsidiaries, overseas servers, custodians abroad? Any jurisdictions with strict local rules? 40 · Is there a live data-protection dimension already: a breach, an ICO interaction, subject access requests from the opponent or departing staff?

§ 12 · QUESTIONS41 - 4 Privilege 41 · Which lawyers have touched these matters: external firms, in-house counsel, and in-house lawyers wearing commercial hats? 42 · Was there an internal investigation, review or report into these events? Who commissioned it, who conducted it, and for what stated purpose? 43 · How does advice travel internally: is legal advice forwarded into business threads, summarised in board packs, pasted into chat? 44 · Is there any joint, shared or common-interest dimension: co-defendants, insurers, group companies sharing advice, prior transactions with shared counsel? adviser?

§ 13 · QUESTIONS46 - 5 Third parties 46 · Which outside organisations hold or process company data: the MSP, hosting and backup providers, payroll, accountants, records storage? Where did the data go at exit? the correspondence? 49 · Are there carriers, banks or

platforms whose records may matter: call records, payment flows, platform accounts and their logs? 50 · Is any other proceeding, regulator or authority already touching this data: police, a regulator, an insurer's investigators, parallel litigation?

§ 14 · C ON VERSION After the meeting: converting answers into actions ANSWER CLUSTER IMMEDIATE OUTPUT FEEDS INTO

§ 15 · ESCALATIONTRIGGERS Red-flag answers THE ANSWER THE SAME-DAY ACTION

§ 16 · WHEREITGOESWRONG & DRAFTING AIDS Common mistakes · Suggested wording Common mistakes Suggested wording · Meeting request to the client (core paragraphs) Suggested wording · Post-meeting c on firm at i on request (core paragraphs)

§ 17 · QUICK CONTROL Checklist · When to involve a digital forensic expert The first-meeting checklist When to involve a digital forensic expert

§ 18 · COMMON QUESTIONS Frequently asked questions Who should attend the first meeting? What if IT is fully out sourced? What if the client cannot answer many of the questions? How long does this take, and can it be split? Should we run this meeting pre-action? Is this meeting privileged, and does the note get disclosed?

§ 19 · REFERENCE Glossary MSP 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

Who should attend the first meeting?

Three roles, ideally under six people: the client's decision-maker (GC or instructing director), whoever actually administers the systems (the in-house IT head or the MSP's lead engineer, specifically not just the account manager), and one operationally senior person close to the events. Individual custodians come later, separately and deliberately so: the strategic meeting and the custodian interviews surface different things.

What if IT is fully out sourced?

Then the MSP is in the meeting (under confidential it y cover), because half the fifty questions are theirs to answer, and the MSP also receives a preservation notice as a third party holding client data. Establish in the meeting who at the provider will implement holds and suspensions, on whose instruction, and confirm the contract's access and assistance terms are being gathered.

What if the client cannot answer many of the questions?

Expect it, and treat the gaps as findings: every "we would have to check" becomes a numbered follow-up with an owner and a date, and the gap pattern itself tells you how much identification support the matter needs. What must not happen is unanswered questions silently becoming unasked ones; the numbered record prevents exactly that.

How long does this take, and can it be split?

Ninety minutes covers the fifty questions at strategic depth with a disciplined chair. Splitting works if the split is by section with the urgent ones first: architecture, custodians, devices, deleted data, retention and preservation (Q1 to 35) cannot wait; privacy, privilege and third parties (Q36 to 50) can follow within days if they must. What cannot be split off is the day-one action list.

Should we run this meeting pre-action?

Yes, when ever a dispute is realistically contemplated: the preservation duties are already live, the volatile data is already dying, and pre-action versions of the fifty questions improve the letter of claim or response as well as the eventual disclosure. The only adjustment is emphasis: pre-action, questions 21 to 35 (deletion, retention, preservation) carry even more weight because more time remains to act on the answers.

Is this meeting privileged, and does the note get disclosed?

The meeting and its note are litigation-privileged legal work in the ordinary way. What the exercise later deploys is derived material: the data map, the hold register, the DRD descriptions and, where identification methodology is probed, the fact that a structured process was followed on stated dates. Structure the note so the factual answers are severable from strategic commentary, and deployment stays clean. 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 20 of 23