

BYOD And Disclosure

This guide for UK lawyers explains how to handle work data on personal devices, covering control, collection routes, and privacy. It details targeted collection protocols, addresses common issues like leavers and wiped devices, and provides practical advice for managing BYOD disclosure.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30. <https://e-discovery.uk/library/byod-and-disclosure>

BYOD & DISCLOSURE · A GUIDE FOR UK LAWYERS BYOD and Disclosure Personal Devices, Work Data and the Collection Nobody Signed Up For COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
PRIVACY-SCOPED EXTRACTION PROTOCOLS 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 company's evidence on the employee's phone 03 Control: when personal-device data is disclosable 04 The routes: consent, contract, compulsion 05 Targeted collection: taking the work, leaving the life 06 Privacy, proportionality and the device owner's rights 07 Leavers, refusers and wiped devices 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:
WORKDATAONPERSONALDEVICESISUSUALLYDISCLOSABLE, RARELYSEIZABLE,
ANDALWAYSCOLLECTABLEWITHTHERIGHTPROTOCOL: THECRAFT IS THE PROTOCOL

§ 02 · FIRST PRINCIPLES The problem in plain English: the company's evidence on the employee's phone

§ 03 · CONTROL Control: when personal-device data is disclosable

§ 04 · THEROUTES The routes: consent, contract, compulsion

§ 05 · THESCALPEL Targeted collection: taking the work, leaving the life

§ 06 · RIGHTS Privacy, proportionality and the device owner's rights

§ 07 · THE HARD CASES Leavers, refusers and wiped devices

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE
DEVICE SYSTEM S / WORK COMPUTER PERSONAL CORPORATE MDM / CLOUD &
(TARGETED) TENANCY PROFILE BACKUPS COUNTERPART DELETED / DEVICES
RECOVERABLE

§ 09 · IN THE WILD Worked examples EXAMPLE1 ·
THEPROTOCOLTHATTURNEDAREFUSALINTOAYES EXAMPLE2 ·
THEDISCLOSURESTATEMENTTHATFORGOTTHEPHONES EXAMPLE3 ·

THEEXITWIPEANDTHECONTAINERTHATLOGGEDIT

§ 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 · CUSTODIANCONSENTPROTOCOL (CORETERMS)

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

§ 13 · COMMON QUESTIONS Frequently asked questions Can my client require an employee to
hand over their personal phone? Is Whats App on a director's personal phone within the
company's control? What if the custodian's phone also holds another employer's confidential
data? Our custodian left the company last year and will not cooperate. Options? Does GDPR
prevent BYOD collection? What should a BYOD policy say to make disclosure workable?

§ 14 · REFERENCE Glossary BYOD MDM 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

Can my client require an employee to hand over their personal phone?

Framed as the handset: rarely, and unwisely. Framed as the work data: usually, via control, contract and reasonable instruction: delivered through the protocol route that takes the data without the device-as-such: Example 1's construction. The distinction is the whole game: demands drafted around data and protocol succeed; demands drafted around the object generate resistance and claims. And where the employee still refuses, §4's ladder and the inference record answer it.

Is Whats App on a director's personal phone within the company's control?

For work threads, commonly yes: directors' duties, service agreements and the practical-ability limb make the company's case strong, and the courts have repeatedly proceeded on that footing in commercial disputes: the disclosure statement should address it expressly. The personal threads around them are not: which is why the collection answer is always the targeted protocol, never the full image to the company's advisers.

What if the custodian's phone also holds another employer's confidential data?

A real and growing wrinkle: consultants and portfolio executives carry several employers per handset. The protocol handles it: app and participant scoping confines the take; the examiner-intermediary keeps third-party confidential material from the instructing party; and where a specific conflict is known, the protocol names it and the filters exclude it. The alternative: wholesale collection into a rival's solicitors: is the breach every one spends the rest of the case regretting.

Our custodian left the company last year and will not cooperate. Options?

In order: the corporate copy (what synced before exit: tenancy, MDM container, backups); surviving contractual duties invoked in correspondence; the counterpart layer (the threads' other ends, per guides 63-65); third-party disclosure against the leaver if the material justifies it; and the refusal chronology feeding inference against whoever benefits from the gap. Prospectively: the exit protocol of §7 is the answer, adopted this quarter, so the next leaver's phone is collected before the badge comes back.

Does GDPR prevent BYOD collection?

No: it disciplines it. Legal-claims necessity and legitimate interests provide lawful bases; minimisation demands the targeting this guide teaches anyway; transparency is delivered by the protocol documents; and the household's data is protected by filter in g that never lets it reach the parties. Collections fail GDPR analysis when they are indiscriminate: which is also when they fail proportionality, custodian relations and judicial patience: the law and the craft point the same way.

What should a BYOD policy say to make disclosure workable?

Five clauses: consent to targeted forensic collection under an independent-examiner protocol when legally required; cooperation with preservation instructions including suspension of deletion settings; exit protocol: work data collected, sync revoked, state documented before departure; MDM or work-profile enrolment where the role justifies it; and transparency about

all of it, because consents extracted obscurely fail when tested. An after no on of drafting against this list converts BYOD from a litigation hazard into an administered estate: the cheapest disclosure improvement most companies can buy. 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

Source: <https://e-discovery.uk/library/byod-and-disclosure>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.