COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

BYOD and Disclosure

Personal Devices, Work Data and the Collection Nobody Signed Up For

Bring Your Own Device stopped being a policy question years ago: it is simply how work happens. The company's deals are negotiated on directors' personal WhatsApp, its documents cached on family iPads, its emails synced to phones the company neither owns nor controls: until a dispute arrives and the personal phone becomes the best evidence in the case. BYOD disclosure sits at the junction of three bodies of law that pull in different directions: the disclosure duties that reach documents within a party's control wherever they sit, the data protection and privacy rights of the device's owner and their family, and the employment relationship that shapes what can be demanded of whom. This guide gives UK lawyers the working framework: when personal-device data is within a party's control, how to collect from devices the company cannot seize, targeted collection methods that take the work data and leave the personal life, the consent and compulsion routes with their limits, and the policies that make the next dispute's BYOD problem smaller than this one's.

⏱ Estimated reading time: 27 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. BYOD collection is among its most frequent instructions: targeted, privacy-respecting extraction from personal devices under consent protocols and court orders, work-data scoping that survives challenge from both directions, and the examiner-intermediary model that lets custodians cooperate without surrendering their private lives. Its eDiscovery arm, **e-discovery.uk**, processes the collected slice into disclosure.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | BYOD & PERSONAL-DEVICE COLLECTION | PRIVACY-SCOPED EXTRACTION PROTOCOLS | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: WORK DATA ON PERSONAL DEVICES IS USUALLY DISCLOSABLE, RARELY SEIZABLE, AND ALWAYS COLLECTABLE WITH THE RIGHT PROTOCOL: THE CRAFT IS THE PROTOCOL

Three propositions frame every BYOD matter. **First, control:** under CPR 31 and PD 57AD, documents are disclosable if within a party's control: and work communications on an employee's personal device commonly are, via the employment relationship, contractual rights (device policies, cooperation clauses), or the practical reality that the party can obtain them by asking: so "it's on his personal phone" is the beginning of the analysis, not its end: the company's disclosure statement must grapple with the BYOD estate, and opponents' statements that ignore it are challengeable. **Second, the seizure gap:** control for disclosure purposes does not make the company owner of the handset: it cannot lawfully image an employee's personal phone wholesale without consent or order, and heavy-handed demands generate ET claims, UK GDPR exposure and unusable collections: the gap between "we are entitled to the work data" and "we may take the phone" is where BYOD disputes combust. **Third, the protocol bridge:** the gap is bridged by targeted collection under documented protocols: scope agreed or ordered (apps, accounts, date ranges, custodial search terms), extraction by an independent examiner who filters at the point of collection, personal material never leaving the custodian's sphere unreviewed, and the methodology recorded so both the employee (privacy) and the opponent (completeness) can test it: the examiner-intermediary model that has become the UK standard precisely because it gives courts a proportionate order to make and custodians a tolerable process to accept. Around these sit the practical layers this guide works through: the consent conversation and its documentation (guide 62's protections applied to the willing); contractual foundations that make the next case easier (BYOD policies with imaging consent, exit protocols that collect before wiping); the compulsion ladder for refusers (orders against parties and employees, with adverse inference filling gaps); leaver and wiped-device scenarios (where guide 61's ecosystem and guide 65's lineages usually rescue what the handset withheld); and the corporate-copy principle: work data that synced through company systems (M365, Google, MDM-managed apps) is collected server-side without touching anyone's phone: the first question, always, being what the servers already hold.

- **Server-side first:** if the work data synced through company systems, collect it there: the phone question shrinks to what only the phone holds.
- **Control reaches, ownership does not:** plead and demand on control; collect by consent, contract or order: never by seizure of what the company does not own.
- **The protocol is the product:** scoped, examiner-mediated, documented extraction: the model both sides and the court can live with.
- **Refusal has consequences:** the compulsion ladder plus inference: a custodian's "no" is managed, not accepted as the end.
- **Policy now, ease later:** BYOD terms with imaging consent and exit collection convert next year's crisis into this year's routine.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the company's evidence on the employee's phone

The modern deal is negotiated in three places at once: the email system the company controls, the meeting platforms it licenses, and the WhatsApp thread on the sales director's personal iPhone: and the candid version usually lives in the third. When the dispute arrives, the company owes disclosure of relevant documents within its control; the director owns the phone, half the data is his family's, and nobody wrote down what happens now. Multiply by every custodian, add leavers who took their phones with them, and BYOD becomes most commercial matters' hardest collection problem: not technically (the extraction is routine) but jurisdictionally: whose data, whose device, whose duty, whose rights.

The resolution this guide teaches is sequencing: establish what company systems already hold (often more than assumed: synced mail, backed-up chats via corporate accounts, MDM-managed app data); define the residue that only personal devices hold; then run the protocol route: consent sought properly, contract invoked where it exists, orders obtained where needed: with targeted extraction throughout, because the collection that respects the custodian's private life is also the collection that survives challenge, wins cooperation, and keeps the tribunal's sympathy where it belongs.

§ 0 3 · CONTROL

Control: when personal-device data is disclosable

- **The control tests:** physical possession, a right to possession, or a right to inspect or take copies: work communications on personal devices frequently satisfy the second or third via the employment contract, device policies, or the employer's practical ability to require production: analysed custodian by custodian, documented in the disclosure statement.
- **Current employees:** the strongest control case: duties of cooperation (express or implied), policy consents, and the practical reality of the relationship: control is the norm, and disclosure statements should say how BYOD sources were addressed.
- **Leavers:** control weakens with the relationship's end: surviving contractual duties (cooperation clauses, confidentiality), the leaver's own party status if joined, and third-party disclosure routes (CPR 31.17) fill the gap: the exit-protocol point of §7 exists because this analysis is easier to avoid than to win.
- **Mixed-use nuance:** control attaches to the work documents, not the device or the personal estate around them: the scoping consequence drives §5's targeted methods.
- **The opponent's BYOD estate:** the same analysis run in reverse: their disclosure statement questioned on personal-device sources, their custodians' WhatsApp within their control just as yours is: §11's questions make the challenge routine.

§ 0 4 · THE ROUTES

The routes: consent, contract, compulsion

- **Consent, done properly:** the preferred route: informed, written, scoped, revocable-in-form but stabilised by the protocol's protections (examiner intermediary, personal-data filtering, return/destruction terms): guide 62's consent craft for the cooperative custodian: most BYOD collections run here, because the protocol makes yes easy.
- **Contract:** BYOD policies with imaging and cooperation consents, employment terms requiring assistance with proceedings, exit undertakings: invoked as the basis for the ask and the answer to reluctance: their absence is the gap §7's policy work closes for next time.
- **Compulsion against parties:** orders for specific disclosure reaching BYOD sources, imaging orders on the guide 35 model (independent examiner, protocol-bound), and the disclosure-statement pressure that makes BYOD silence untenable.
- **Compulsion against non-parties:** employees who are not parties reached via the employer's control, or directly by third-party disclosure and witness machinery: slower, used when the relationship routes fail.
- **Inference for the gap:** where a custodian refuses and compulsion is disproportionate or defeated, the refusal itself: documented, chronologised: feeds the adverse-inference case: guide 62 §4's structure, BYOD edition.

§ 0 5 · THE SCALPEL

Targeted collection: taking the work, leaving the life

- **Scope before tooling:** the protocol defines targets: named apps (WhatsApp, mail clients, Slack), named accounts, date ranges, participant lists: agreed between parties or ordered: the extraction then serves the scope, not the tool's appetite.
- **Targeted and app-level extraction:** modern tooling supports app-scoped and account-scoped acquisition (guide 61 §2's targeted tier): where forensic questions (deletion, integrity) demand deeper images, the protocol pairs depth with filtering: full extraction to the examiner, scoped production onward: nothing personal reaching the instructing party unreviewed.
- **The examiner intermediary:** the independent laboratory holds the device data, applies the filters (date, app, participant, search terms), routes responsive work material to review, and returns or destroys the rest under the protocol's terms: the model courts order because it works.
- **Family and third-party data:** the phone holds the household: partners' messages, children's photos, medical and financial life: the protocol's filtering exists for them, and the UK GDPR analysis (§6) is written with them in mind.
- **Documentation throughout:** what was extracted, what filters ran, what was produced, what was excluded and why: the record that answers both challenges: the custodian's "they took everything" and the opponent's "they left things out".

§ 0 6 · RIGHTS

Privacy, proportionality and the device owner's rights

- **UK GDPR applies throughout:** collection is processing: lawful basis identified (legitimate interests balanced, legal-claims necessity), minimisation honoured by the targeting of §5, transparency delivered through the protocol documents, and DPIA-style thinking for large custodian populations.
- **Article 8 and the household:** the private and family life on the handset weighs in every proportionality balance: courts scope orders accordingly, and collection plans that pre-shrink themselves fare better than maximalist demands cut down.
- **Employment law's frame:** trust-and-confidence, reasonable instructions, and the ET consequences of overreach: the demand letter drafted with the employment team, not around it.
- **Special category and third-party spillover:** health data, union membership, others' correspondence: identified as risks in the protocol, filtered by default, handled under confidentiality terms where responsive despite it all.
- **Proportionality both ways:** the device's evidential centrality justifies more; peripheral custodians justify less: the dial from this series' proportionality method, applied per phone: and recorded, because the reasons are the defence.

§ 0 7 · THE HARD CASES

Leavers, refusers and wiped devices

- **Leavers:** the control analysis weakens, the phone walks out, and the corporate copy becomes the estate: which is why exit protocols (collect work data before departure, revoke sync, document the state) belong in every BYOD policy: for the current case, surviving duties, party joinder and third-party routes per §3.
- **Refusers:** the compulsion ladder of §4 run with its costs weighed: and the refusal chronology built regardless: dated requests, protocol offers declined, protections rejected: the record that makes inference natural and costs orders likely.
- **Wiped and reset devices:** guide 61's honest position: the reset is usually effective device-side and loud ecosystem-wide: backups, synced accounts, counterpart devices and corporate copies survive it, and the wipe's own timing joins the conduct case: the BYOD wipe after a preservation letter is among the most self-defeating moves in modern disclosure.
- **Lost and replaced phones:** the lineage questions of guide 65 §11: backups, peers, the replacement device's restored state: "lost" ends the handset, not the estate.
- **MDM and containerisation:** where the employer ran mobile device management or work profiles, the managed container is corporate-side collectable: its logs date sync and wipe events, and its existence shrinks the personal-device residue: the first document requested in any BYOD dispute is the MDM posture.

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the personal phone is one node in an estate the company partly holds already. BYOD evidence also lives in: corporate servers and tenancies (mail, Teams/Slack, document systems) where work data synced; MDM and work-profile containers with their logs; cloud accounts (personal and corporate) backing up the device; computer backups on home and work machines; counterpart devices holding the other end of every thread (guides 63-65's standing rescue); the custodian's other devices (tablets, old phones, desktops with linked sessions); and the corporate paper trail around the BYOD relationship: policies, consents, exit records: which frame every dispute about what could be demanded. The collection plan starts server-side, shrinks the phone question to the residue, and walks this map for whatever the handset withholds.

EVIDENCE	PERSONAL DEVICE (TARGETED)	CORPORATE SYSTEMS / TENANCY	MDM / WORK PROFILE	CLOUD & COMPUTER BACKUPS	COUNTERPART DEVICES	DELETED / RECOVERABLE
Work email	Synced copies + cache	Y: collect here first	Managed-app data	In device backups	Recipients' copies	Server retention rules govern
WhatsApp / personal-channel work chats	Y: the core residue	Rarely (unless business API)	Sometimes containerised	Y: lineages	Y: every participant	Guide 63's layers
Documents / files	Local copies, app caches	Y where synced (OneDrive etc.)	Container storage	Y	Shared recipients	Version stores server-side
Sync / wipe events	Device logs	Tenancy sign-in logs	Y: the event record	Backup timestamps	n/a	Logs outlive the wipe
Policy / consent record	n/a	HR and policy systems	Enrolment records	n/a	n/a	The dispute's frame

Fallback strategy in one line: collect the corporate copy first, the counterpart copies second, the lineages third: and let the phone's role shrink to what only it ever held.

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE PROTOCOL THAT TURNED A REFUSAL INTO A YES

A finance director refused point-blank to hand his personal iPhone to his employer's solicitors in a fraud investigation: "my divorce is on that phone". The instruction shifted to the protocol model: an independent laboratory would extract, only three apps within a fourteen-month window would be filtered, participant lists would confine the take to the counterparties in issue, everything else would be destroyed under undertaking, and he could attend the extraction. He agreed within a week: the targeted collection produced ninety-one responsive WhatsApp threads, none of his personal life reached the company, and his cooperation: recorded in the protocol's schedule: later served him well on costs. The refusal had never been about the evidence; it was about the divorce: and the protocol was built to believe him.

EXAMPLE 2 · THE DISCLOSURE STATEMENT THAT FORGOT THE PHONES

A defendant company's disclosure statement listed its M365 tenancy and file servers: no BYOD sources, despite pleadings describing deal negotiations "by WhatsApp". The claimant's application under PD 57AD was short: the custodians' own produced emails referenced WhatsApp threads; the company's BYOD policy (disclosed in the HR bundle) contained imaging consents; control was therefore arguable and unaddressed. The court ordered the statement remade with personal-device sources addressed custodian by custodian, and targeted collection under a protocol for four individuals. The threads recovered included the renegotiation messages the claim needed. The lesson the judgment states expressly: a disclosure statement that ignores the BYOD estate in a case pleaded on personal-channel communications does not comply with the duty.

EXAMPLE 3 · THE EXIT WIPE AND THE CONTAINER THAT LOGGED IT

A departing head of sales wiped his personal phone the evening before returning his access badge: and with it, the employer assumed, the client-diversion messages it suspected. The estate disagreed: the MDM work profile had logged its own removal at 19:42 with the device identifier; the corporate container's last sync, four days earlier, had captured his managed-mail drafts including two to the competitor; his OneDrive sync history showed the pricing folder accessed from the device that week; and the counterpart layer: two clients who cooperated: produced the WhatsApp threads his wipe had removed from only one of their ends. The wipe erased his copy and created the timeline's centrepiece: 19:42, badge return at 09:00: and the speedy trial judgment reads the hour as intent.

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Seizure instincts:** demanding the handset wholesale: the combustion point of §1's second proposition: cooperation lost, claims generated, collections tainted.
- **BYOD-blind disclosure statements:** Example 2's omission: personal-device sources unaddressed in cases pleaded on them.
- **Server-side skipped:** phones fought over while the tenancy held the synced copy all along.
- **Protocols improvised:** scoping, filtering and destruction terms invented mid-collection: challenge invited from both directions.
- **Leaver data uncollected at exit:** the walk-out problem accepted annually and solved never.
- **Refusals accepted flat:** no ladder run, no chronology built, no inference laid.
- **Family data mishandled:** household material reaching the instructing party unfiltered: the breach that poisons everything after it.
- **MDM posture unasked:** the container's corporate-side copy and event logs discovered late or never.

Technical limitations

- **Targeted extraction has floors:** some acquisitions are all-or-filtered-after, not scoped-at-source: the protocol's filtering layer exists because tooling granularity varies by platform and version.
- **Personal-channel deletion behaves per its app:** guides 63-65 govern: BYOD adds the access question, not new recovery physics.
- **Control is argued, not assumed:** the legal analysis varies with contracts, policies and relationships: the technical plan waits on it.
- **MDM sees the container, not the phone:** corporate visibility ends at the work profile's wall: personal-side artefacts still need the protocol route.
- **Consent collections depend on the consent holding:** revocation mid-process is managed by protocol terms and, where needed, the order that replaces agreement.

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- The BYOD census: which custodians do work on personal devices, on which apps: and what do corporate systems already hold of it?
- The paper: BYOD policy, imaging consents, exit protocol, MDM posture: what exists, and what does it let us ask for?
- Any leavers, refusers or wiped devices already: and is the chronology being built?

Ask your opponent

- Please confirm your disclosure statement addresses personal devices used for relevant communications, custodian by custodian, stating the control analysis applied.
- Please identify all custodians who used personal devices or personal-channel apps for relevant business, the MDM or work-profile posture for each, and the steps taken to preserve and collect from those sources.
- Where any custodian has left, refused, or wiped or replaced a device: please give particulars and the dates.

Ask your eDiscovery / forensic provider

- What does server-side collection already cover, and what residue genuinely needs the phones?
- What protocol: scope, filters, intermediary terms: fits these custodians and this court?
- For the wiped or withheld device: what does the §8 map recover, and what does the event record date?

SUGGESTED WORDING · CUSTODIAN CONSENT PROTOCOL (CORE TERMS)

> "The custodian consents to the extraction of data from the device by [laboratory], an independent forensic examiner, on the following terms: (1) extraction shall be conducted by the examiner and no image or extraction shall be provided to [the company] or its advisers; (2) the examiner shall apply the agreed filters, being [apps], [date range] and [participants/search terms], and only material within them shall be reviewed for relevance and produced; (3) all other data shall be retained securely by the examiner solely for integrity-verification purposes until [date/event], then destroyed, with confirmation in writing; (4) the custodian may be present or represented at extraction and shall receive a copy of the extraction record; and (5) nothing in this protocol constitutes consent to any wider access, and the custodian's personal data shall be processed only as described, in accordance with UK GDPR."

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The BYOD checklist

- ☐ BYOD census run at matter-open: custodians, apps, devices, MDM posture
- ☐ Server-side collection scoped first; phone residue defined honestly
- ☐ Control analysis documented per custodian; disclosure statement addresses it
- ☐ Consent sought protocol-first; contract terms invoked where they exist
- ☐ Targeted extraction scoped: apps, dates, participants: and recorded
- ☐ Examiner-intermediary model engaged; filtering before anything moves
- ☐ UK GDPR basis, minimisation and transparency documented
- ☐ Leaver exits collected; refusal chronologies built; wipe events dated
- ☐ Counterpart and lineage routes mapped for withheld devices
- ☐ Opponent's BYOD estate interrogated per §11

Red flags

- Disclosure statements silent on phones in personal-channel cases: Example 2.
- Wipes, resets or "lost" devices dated to notice: Example 3's hour.
- Wholesale imaging demands where targeted routes were offered.
- MDM removal or sync revocation events mid-dispute.
- Refusals with no protocol ever offered: on either side.
- Personal data of custodians' families handled outside any protocol.
- Exit processes that return badges and ignore data.

When to involve a digital forensic expert

At the census, where the server-side/residue split decides scale; at protocol design, where scope, filters and intermediary terms must satisfy custodian, opponent and court at once (Example 1's construction); at execution, where targeted extraction, filtering and documentation are the laboratory's core craft; and at the hard cases, where wiped devices, leavers and refusers are worked through the §8 map and the event record (Example 3's estate). Reported under CPR Part 35 with scopes and filters stated: and through **e-discovery.uk**, the collected slice is processed into review beside the corporate estate, deduplicated and threaded per guides 82-83.

§ 13 · COMMON QUESTIONS

Frequently asked questions

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 WhatsApp 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 everyone 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 filtering 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 afternoon of drafting against this list converts BYOD from a litigation hazard into an administered estate: the cheapest disclosure improvement most companies can buy.

§ 14 · REFERENCE

Glossary

BYOD
Bring Your Own Device; personal hardware carrying work data.

Containerisation
Separated work profile on a personal device; the corporate-visible zone.

Control (CPR 31.8)
Possession or rights to possession, inspection or copies; the disclosability test.

Examiner intermediary
The independent laboratory holding data and applying filters between custodian and party.

Exit protocol
Pre-departure collection, sync revocation and state documentation.

MDM
Mobile device management; corporate administration of enrolled devices or profiles.

Residue (BYOD)
Work data existing only on the personal device after server-side collection.

Targeted extraction
App-, account- and date-scoped acquisition; the scalpel of §5.

Wipe event
The logged reset or profile removal; datable, and read as conduct when timed to notice.

Work profile
Android/iOS managed partition; MDM's unit of visibility.

Sources and authoritative references

The BYOD collection disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (targeted personal-device collection, examiner-intermediary protocols, wipe-event analysis, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 01 · Identification, Phase 02 · Preservation and Phase 03 · Collection (BYOD census; protocol collection into review): e-discovery.uk/edrm/identification · e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- PD 57AD and CPR Part 31: justice.gov.uk, PD 57AD · justice.gov.uk, Part 31 · CPR Part 35: justice.gov.uk, Part 35
- ICO, employment practices and UK GDPR guidance: ico.org.uk
- ISO/IEC 27037: iso.org, 27037 · College of Policing, device extraction guidance: college.police.uk

DISCLAIMER

This publication provides general information about BYOD and disclosure as at August 2026. Control analyses turn on specific contracts, policies and relationships; platform, MDM and extraction capabilities change frequently; verify the current position for the matter at hand. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

BYOD instructions at the laboratory run the sequence this guide teaches: the census and server-side scoping that shrink the phone problem; protocol design that custodians accept and courts order (Example 1's model, drafted with both audiences in mind); targeted extraction with examiner-intermediary filtering as standard; and the hard-case work: wipe events dated from MDM and sync logs (Example 3's 19:42), leavers' estates rebuilt from corporate copies and counterparts, refusal chronologies documented for the inference case. Reporting is CPR Part 35 with scopes, filters and methods stated; through **e-discovery.uk**, the collected residue is processed, deduplicated and threaded into the wider review. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if a departing custodian's phone is leaving the building this week, the exit collection call comes first.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace