Electronic Disclosure Explained A Practical Guide For UK Lawyers

Electronic disclosure in UK litigation involves identifying, preserving, collecting, processing, reviewing, producing, presenting, and disposing of electronically stored information. This guide covers the legal duties, rules, and sanctions, alongside practical advice for managing e-disclosure effectively in England and Wales.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-29.
https://e-discovery.uk/library/electronic-disclosure-explained-a-practical-guide-for-uk-lawyers

ELECTRONICDISCLOSURE · A GUIDE FOR UK LAWYERS Electronic Disclosure Explained A Practical Guide for UK Lawyers COMPUTER FORENSICS LAB DISCOVERY. UK

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

§ CONTENTS In this guide 01 Executive summary 02 What exactly is electronic disclosure? The problem in plain English 03 How e Disclosure differs from simply exchanging documents 04 e Disclosure and its neighbours: forensics, review and information governance 05 Why it matters legally: duties, rules and sanctions 06 The legal framework: England & Wales, and where the rules differ 07 Important terminology 08 The complete lifecycle: identification to disposal 09 Practical workflow and decision tree 10 Preservation: legal holds done properly 11 Collection methodology and evidential integrity 12 Metadata: the evidence about the evidence 13 Privilege and confidential it y 14 UK GDPR, data minimisation and the Data (Use and Access) Act 15 Proportionality 16 Realistic litigation examples 17 Common mistakes and technical limitations 18 Questions to ask: client, opponent, provider 19 Suggested wording for instructions 20 Checklist and red flags 21 When to involve a digital forensic expert 22 Frequently asked questions 23 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary SEVEN POINT S TO HOLD ON TO 31 and PD 31B govern most other civil claims. Know which applies before the first case management THEONE - SENTENCEVERSION

§ 02 · FIRST PRINCIPLES What exactly is electronic disclosure? The problem in plain English IDENTIFICATION PRESERVATION COLLECTION PROCESSING REVIEW & PRODUCTION PRESENTATION DISPOSAL ANALYSIS

§ 03 · THECOREDISTINCTION How e Disclosure differs from simply exchanging documents FOR THE PRACTITIONER DIMENSION "SIMPLY EXCHANGING DOCUMENTS" EDISCLOSURE DONE PROPERLY

§ 04 · THE MAP OF THE TERRITORY e Disclosure and its neighbours e Disclosure vs ordinary document disclosure e Disclosure vs digital forensics e Disclosure vs document review e Disclosure vs information governance DISCIPLINE CORE QUESTION T YPICAL OUTPUT GOVERNING FRAMEWORK

§ 05 · CONSEQUENCES Why it matters legally: duties, rules and sanctions The duties The

sanctions FAILURE REALISTIC CONSEQUENCES

§ 06 · THE RULES The legal framework: England & Wales, and where the rules differ Civil claims in the Business and Property Courts: PD 57AD CURRENTSTATUS · Civil claims outside the B&PCs: CPR Part 31 and PD 31B Criminal proceedings Where the rules differ FORUM KEY DIFFERENCES FROM E&W CIVIL DISCLOSURE

§ 07 · VOCABULARY Important terminology TERM WHAT IT MEANS IN PRACTICE

§ 08 · THELIFECYCLE The complete lifecycle: identification to disposal Stage 1 · Identification Stage 2 · Preservation Stage 3 · Collection Stage 4 · Processing Stage 5 · Review and analysis Stage 6 · Production Stage 7 · Presentation Stage 8 · Disposal

§ 09 · IN PRACTICE Practical workflow and decision tree The first fourteen days of a new dispute Decision tree: scoping the exercise QUESTION1 YESNO, INVESTIGATION ONLY QUESTION2 B & PCCIVILCLAIMOTHERCIVILCLAIMCRIMINAL / REGUL AT ORY / CMC. ARBITRAL QUESTION3 WHEN ACTION YESNO QUESTION4 SMALL (< ~ 20KDOCUMENTS) LARGE QUESTION5

§ 10 · FREEZINGTHERECORD Preservation: legal holds done properly WH AT ADEFENSIBLEHOLDLOOKSLIKE

§ 11 · DEFENSIBLE CAPTURE Collection methodology and evidential integrity Choosing the method Chain of custody INTEGRITYINONEPARAGRAPH METHOD APPROPRIATE FOR WATCH-POINTS

§ 12 · BENEATHTHESURFACE Metadata: the evidence about the evidence T YPE EXAMPLES LITIGATION USE

§ 13 · PROTECTEDMATERIAL Privilege and confidential it y

§ 14 · UK GDPR, data minimisation and the Data (Use and Access) Act

§ 15 · Proportionality

§ 16 · IN THE WILD Realistic litigation examples EXAMPLE1 · THESHAREHOLDERDISPUTEANDTHEWHATSAPPTHREAD EXAMPLE2 · THEBACKDATEDCONSULTANCYAGREEMENT EXAMPLE3 · THELEAVERANDTHECLIENTLIST

§ 17 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations to understand (and explain to clients)

§ 18 · INTERROGATORIES Questions to ask Ask your client Ask your opponent (in DRD/EDQ exchanges or correspondence) Ask a forensic / e Disclosure provider

§ 19 · DRAFTING AIDS Suggested wording for instructions LEGALHOLDNOTICE (COREOPER AT IVE PA R AG RAPHS) INSTRUCTION TO AN EDISCLOSURE / FORENSIC PROVIDER PROPOSALTOTHEOPPONENTONPRODUCTIONFORM AT (FOR THE DRD / EDQ)

§ 20 · QUICK CONTROL Checklist and red flags The e Disclosure checklist Red flags

§ 21 · ESCALATION When to involve a digital forensic expert

§ 22 · COMMON QUESTIONS Frequently asked questions What is e Disclosure, and how is it different from simply exchanging documents? Do we need an e Disclosure exercise in a small case? Can we just print the Whats Apps / take screenshots? Is technology-assisted review accepted by the courts? Who pays for all this? What happens to the data when the case ends?

§ 23 · REFERENCE Glossary DRD EDQ EDRM ESI EXIF TAR Authoritative UK 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

What is e Disclosure, and how is it different from simply exchanging documents?

e Disclosure is the defensible process for per form in g disclosure on electronically stored information: identifying and preserving sources, collecting them without damaging metadata, processing and culling the volume, review in g for relevance and privilege, and producing in agreed formats with an audit trail. Simply exchanging documents is only the last step of that chain, performed without the process that makes it complete, verifiable and safe to certify. The rules (PD 57AD; PD 31B) assume, and in places require, the process, not just the exchange.

Do we need an e Disclosure exercise in a small case?

You always need the duties discharged, preservation, honest search, accurate certification. The machinery scales: a two-custodian dispute may need only a hold notice, a documented mailbox export and a small review database. What never scales down is self-collection by the client and unpreserved phones.

Can we just print the Whats Apps / take screenshots?

Screenshots prove that pixels existed on a screen; they carry no metadata, omit context, and are trivially fabricated, courts and tribunals increasingly say so. Extract chat evidence forensic all y from the handset or backup so completeness and integrity can be demonstrated.

Is technology-assisted review accepted by the courts?

Yes. English courts approved predictive coding in Pyrrho (2016) and have treated it as unexceptional since; PD 57AD's DRD asks parties to state whether they will use analytics and TAR, and larger parties may be pressed to justify not using it. The defensibility question has moved from "may we?" to "how was it validated?"

Who pays for all this?

Each party generally bears its own disclosure costs, subject to costs budgeting and the ultimate costs order, but disproportionate demands can be met with applications to shift or cap costs, and disclosure conduct (good and bad) is regularly reflected in costs awards. The cheapest lever remains scope: custodians, dates and sources.

What happens to the data when the case ends?

It should be returned or verifiably destroyed under the provider contract and the client's retention policy, subject to any surviving obligation (appeal windows, related proceedings, regulatory holds). Indefinite hosting of a litigation database full of third-party personal data is a data-protection liability with a monthly invoice attached. 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