

CCTV Evidence

CCTV evidence is time-sensitive and requires immediate action to prevent overwrite. This guide details the recording estate, preservation strategies, export methods, and authenticity considerations for UK litigators, in-house counsel, and investigators. It covers common mistakes, technical limitations, and when to involve a digital forensic expert.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30. <https://e-discovery.uk/library/cctv-evidence>

CCTVEVIDENCE · A GUIDE FOR UK LAWYERS CCTV Evidence Recorders, Retention Loops and the Footage That Overwrites Itself While You Draft the Letter COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
CLOCK & TIMELINE VERIFICATION CPR PART 35 EXPERT REPORT S FULL
CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: evidence on a countdown 03 The recording estate: DVRs, NVRs, cloud cameras and doorbells 04 The preservation race: stopping the overwrite 05 Export and collection: keeping footage evidential 06 Clocks, synchronisation and the timeline 07 Authenticity, enhancement and interpretation 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:
CCTVISWONORLOSTINTHEFIRSTWEEK: PRESERVEBEFORE THELOOP,
EXPORTNATIVELY, VERIFYTHECLOCK

§ 02 · FIRST PRINCIPLES The problem in plain English: evidence on a countdown

§ 03 · THEESTATE The recording estate: DVRs, NVRs, cloud cameras and doorbells

§ 04 · THERACE The preservation race: stopping the overwrite

§ 05 · GETTINGITOUTINTACT Export and collection: keeping footage evidential

§ 06 · TIME Clocks, synchronisation and the timeline

§ 07 · REAL, CLEAR, ANDFAIRLYREAD Authenticity, enhancement and interpretation 35 and the standing fairness rule.

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE
CENSUS EXPORTS / PRIMARY CLOUD LOGS & DELETED / RECORDER LAYER PERIPHERY
RECOVERABLE OTHER PRIOR CAMERAS COPIES

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THECENSUSTHATBEATTHELOOP
EXAMPLE2 · THEGAPTHATHADASERVICETICKET EXAMPLE3 ·
THECLIPWITHHTWOENCODINGLIVES

§ 10 · WHERE IT GOES WRONG 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 · CCTV LIMB FOR THE PRESERVATION LETTER

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

§ 13 · COMMON QUESTIONS Frequently asked questions How long do businesses actually keep
CCTV? The footage has already been overwritten. Any hope? Is a phone recording of the
CCTV monitor admissible? The other side says our clip is a deepfake. Now what? Can we
enhance the footage to read the number plate? Do we have to redact other people before
disclosing footage?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab
Speak to a forensic examiner, not a salesperson. INSTRUCT THE LAB
NEW ENQUIRIES EMAIL - DISCOVERY

Questions and answers

How long do businesses actually keep CCTV?

Commonly seven to thirty-one days on self-overwriting loops, with cloud plans in similar ranges and doorbells often shorter: but it is a per-system fact, not a rule: which is why every preservation letter asks the retention question expressly and why the census happens the first after no on. Assume the shortest plausible loop and move at its speed.

The footage has already been overwritten. Any hope?

A margin, not a promise: deleted-but-not-overwritten clips, cloud recycle layers and fragment carving from an imaged disc occasionally recover material, and §8's map: other census cameras, copies already exported, the logs and periphery: rebuilds events without the primary pictures. What is genuinely overwritten is gone; what the estate holds else where is usually more than first appears.

Is a phone recording of the CCTV monitor admissible?

Admissible, and vulnerable: it is evidence of what a screen showed, with resolution, frames and metadata lost and provenance questions attached: weight, not admissibility, is where it suffers. Treat it as the emergency rung it is: use it to justify urgent native collection, not as the collection.

The other side says our clip is a deepfake. Now what?

Meet method with method: provenance (native export from an identified recorder, hashes from acquisition, custody unbroken) plus exam in at i on (encoding generations, container consistency, frame and audio continuity) is how genuine footage answers the challenge: and why footage collected per §5 rarely fears it. A reflexive deepfake allegation against documented provenance tends to cost its maker credibility: invite it into the expert channel and let the reports speak.

Can we enhance the footage to read the number plate?

Only if the pixels exist: legitimate enhancement (contrast, stabilisation, frame integration) can clarify marginal detail, and some time s several low-quality frames combine into a readable plate: but nothing lawful invents resolution that was never captured. An examiner will tell you quickly which side of the line your footage sits: ask before pleading what it shows.

Do we have to redact other people before disclosing footage?

Handle, and often redact: footage of identifiable bystanders is personal data: disclosure into proceedings is lawful with proper basis, but UK GDPR minimisation, security and fairness still apply, and blurring uninvolved third parties (especially children) is standard good practice the court will expect. Build redaction time into the video workflow rather than discovering it at bundle stage. 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/cctv-evidence>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.