

Door Access Swipe Cards And Building Logs

Door access, swipe cards, and building logs create a digital diary of physical presence. This guide for UK lawyers explains how to interpret these records, attribute events to individuals, and integrate them into a digital timeline for litigation or investigation, highlighting common pitfalls and expert involvement.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-30.
<https://e-discovery.uk/library/door-access-swipe-cards-and-building-logs>

ACCESS CONTROL EVIDENCE · A GUIDE FOR UK LAWYERS Door Access, Swipe Cards and Building Logs Physical Presence Evidence and What a Badge Event Does and Does Not Prove
COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
TIMELINE CONSTRUCTION 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 building keeps a diary 03 The access-control estate: readers, controllers and platforms 04 What the logs record and how to read them 05 Attribution: card, credential and human 06 Collection and retention: getting the logs before they go 07 Joining presence to the digital timeline 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:
BADGELOGSPLACEACREDENTIALPRECISELY: MAKINGTHEM
PLACEAPERSONISTHEANALYTICALWORK

§ 02 · FIRST PRINCIPLES The problem in plain English: the building keeps a diary

§ 03 · THEESTATE The access-control estate: readers, controllers and platforms

§ 04 · THERECORD What the logs record and how to read them

§ 05 · WHOSE H AND Attribution: card, credential and human

§ 06 · BEFOREITGOES Collection and retention: getting the logs before they go

§ 07 · THEJOIN Joining presence to the digital timeline

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives EVIDENCE
TURNSTILES / CONTROLLERS / CCTV DIGITAL TIME & DELETED / PLATFORM LAYER
PERIPHERY ATTENDANCE RECOVERABLE LIFTS / VISITORS

§ 09 · IN THE WILD Worked examples EXAMPLE1 ·
THEOVERTIMETHATBADGEDITSELFOUT EXAMPLE2 · THESERVERROOMAT02: 12, AND
WHOSE H AND EXAMPLE3 · THEABSENCETHATPROVEDNOTHING, HONESTLY

§ 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 · ACCESS - CONTROLLIMB FORTHE PRESERVATION LETTER

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The access-control checklist Red flags When to involve a digital forensic expert 35. Through e-discovery.uk, the building's diary sits on the same reviewed chronology as everything else the

§ 13 · COMMON QUESTIONS Frequently asked questions How long are swipe logs actually kept? Can badge data alone prove someone was in the building? The logs show no exit for our witness. When did they leave? Our client says a colleague borrowed their card. Hopeless? Is building access data caught by disclosure duties like documents? Can employers freely use this data to investigate staff?

§ 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. INSTRUCTTHELAB NEWENQUIRIES@EMAIL - DISCOVERY

Questions and answers

How long are swipe logs actually kept?

Anywhere from weeks to a few years: it is a configuration and platform fact, not a standard: controller-local buffers are shortest, head-end databases longest, and visitor and alarm layers run their own schedules. The only safe assumption is that a window is closing, which is why the census and the ask happen in week one.

Can badge data alone prove someone was in the building?

It proves the credential was: the person follows from corroboration: CCTV at the reader, biometrics, journey coherence, paired device activity: per §5's ladder, and honest findings say which rung they stand on. Example 2 shows the ladder reaching certainty; a lone badge event never does by itself.

The logs show no exit for our witness. When did they leave?

Possibly unknowable from the doors: free-exit design logs entries only: so departure brackets from the estate's other diaries: turnstiles and barriers, alarm set events, last logins and prints, final Wi-Fi as so c i at i on, car park systems. The bracket is often tight enough to plead; the door log alone was never going to be.

Our client says a colleague borrowed their card. Hopeless?

Testable, both ways: lending is common and some time s true: the exam in at i on checks whose rhythm the events match, hunts simultaneity contradictions (the card here, the holder's login there), reads CCTV at the readers, and hears the alleged borrower. Where the ladder's rungs point away from the holder, the defence stands up; where they converge on them, Example 2 is how it ends.

Is building access data caught by disclosure duties like documents?

Fully: it is recorded information within a party's control, disclosable where relevant and preservable from the moment litigation is contemplated: purging it on schedule after that moment invites the adverse-inference conversation. The practical wrinkle is operational: the data often sits with facilities teams or landlords who have never met a disclosure obligation: hence the §11 letter's forwarding limb.

Can employers freely use this data to investigate staff?

Purposefully, proportionately and transparently: presence data is personal data: investigation use needs a lawful basis, honest privacy notices help, minimisation is expected, and pattern analysis brushing sensitive inferences (health, religion, union activity) deserves particular care and usually a DPIA. Well-run investigations use the data confidently inside those rails: the rails are not the obstacle; ignoring them is. 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/door-access-swipe-cards-and-building-logs>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.