COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

NAS Evidence: The Office Box That Holds Everything

RAID, Snapshots, Shared Access, Logs and Deleted Data on Network-Attached Storage

In small and mid-sized businesses, the NAS in the comms cupboard is the file server, the backup target, the CCTV recorder and sometimes the company's entire documentary history: a consumer-priced appliance from Synology, QNAP or similar carrying enterprise-weight evidence. Collecting from it defensibly means understanding RAID (the data exists only as an assembled array, not on any single disk), appliance snapshots and recycle folders, the unit's own user accounts and logs, and the sync apps and cloud relays that quietly copy its contents elsewhere. This guide covers acquisition options, what a NAS records about access and deletion, the alternative places its evidence also lives, and the mistakes that turn the office box into a lost cause.

⏱ 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. NAS units arrive at the laboratory weekly: seized under order, delivered by owners, or collected on site: including RAID reconstructions from failed and disassembled arrays. Its eDiscovery arm, **e-discovery.uk**, integrates NAS collections into disclosure-scale processing and review.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACPO / NPCC DIGITAL EVIDENCE PRINCIPLES | NAS & RAID ACQUISITION AND RECONSTRUCTION | DELETED DATA RECOVERY | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

§ 0 1 · ORIENTATION

Executive summary

THE HEADLINE POINT: TREAT THE APPLIANCE AS A SMALL SERVER WITH BIG HABITS

A NAS is a computer: its own operating system, user accounts, permissions, logs, snapshot machinery, recycle folders, and apps that sync its contents to clouds, phones and other sites. Everything this series says about file servers (guide 43's three layers: content, history, context) applies, with three appliance-specific twists. **First, RAID:** the data exists only as an array assembled across multiple disks; a single disk out of the box is meaningless stripes, so acquisition is either of the assembled volume (live, over the network or attached storage, to forensic standards) or of every disk individually with laboratory reconstruction: and amateur disk-pulling is how evidence and arrays die together. **Second, the appliance's own records:** NAS operating systems keep user and connection logs, file-access logs where enabled, snapshot series and network recycle bins whose retention the owner rarely knows: the history and context layers, in vendor-specific dress, perishable on vendor-specific schedules. **Third, the quiet copies:** sync clients on office PCs, vendor cloud relays (QuickConnect and equivalents), phone apps, replication to a second unit and USB backup jobs mean NAS contents usually exist in several other places: which is both a preservation duty (name them) and the recovery plan when the box itself is locked, wiped, failed or missing. The lawyer's contribution mirrors guide 43's: the day-one preservation email, the credential hunt (admin login above all), and an instruction that names content, history, context and the alternative paths together.

- **Do not let anyone pull disks:** the commonest catastrophic act; order of removal, slot positions and array metadata matter, and a rebuilt-wrong array can overwrite what it held. Photograph, power down properly if directed, and let the examiner drive.
- **The admin credential is the front door:** appliance examination, snapshot access and log export run through the NAS's own admin account; hunt it on day one (owner, IT, the supplier who set it up, password managers), with encrypted-volume keys close behind.
- **Network recycle bins catch what shares usually lose:** unlike plain Windows shares, NAS appliances often keep deleted files in per-share recycle folders: check before anyone declares destruction.
- **CCTV may live here too:** many units run surveillance apps; footage retention is short and overwrite is continuous: a same-day preservation item when the box doubles as the recorder.
- **Suspend the schedules:** snapshot pruning, recycle emptying, log rotation and backup-job overwrites: one email, adapted from guide 43's, sent today.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: the box nobody documented

The NAS is bought once, configured by whoever was technical that year, and forgotten until it matters. Then the questions arrive at once: What is on it? Who could access it? What was deleted, and when? Where is the admin password? Was it syncing to the departed director's laptop? And, from the examiner: what RAID mode, which firmware, are the volumes encrypted, do the snapshots go back before the dispute? In a company with an IT department these questions have owners; around a NAS they usually have shrugs, and the appliance's evidence is lost not to sophistication but to neglect: a recycle bin on a 30-day timer, snapshots pruned weekly, an office move where the disks were slotted back in the wrong order.

The remedy is speed and humility: preserve first (power state photographed, schedules suspended, nobody touching disks), hunt the admin credential, and get an examiner to the unit (physically or remotely) before routine housekeeping eats the history. The box that looks like an appliance and is treated like a filing cabinet is, in truth, a small server holding the company's memory: this guide is about handling it as such.

§ 0 3 · THE ARRAY

RAID in plain English: why the disks are not the data

- **The idea:** RAID spreads data across several disks for capacity, speed or failure-tolerance: mirroring (two disks, same content), striping with parity (data plus recovery information across three or more), and vendor hybrids. The volume users see is a mathematical assembly of all member disks; no single disk contains readable files.
- **The evidential consequences:** (1) acquisition must capture either the assembled volume or every member disk, in order, with the array's configuration recorded; (2) a missing or failed disk may still leave the array recoverable (that is the point of parity), so "one drive died" is not "the evidence died"; (3) disks separated from their box, unlabelled, are a reconstruction puzzle: solvable in the laboratory from on-disk metadata, but slower and riskier than a documented removal; and (4) initiating a rebuild on suspect hardware can overwrite recoverable material: the reason nobody presses anything before the examiner arrives.
- **Failed and degraded arrays are laboratory work:** imaging each member (including the failing one, sector by sector), reconstructing the array virtually, and mounting the result read-only: routine for a forensic laboratory, fatal for improvisation: the guide 39 kit-list example, at appliance scale.
- **Encryption stacks on top:** encrypted volumes or shared folders require their keys in addition to array assembly; the credential hunt covers both, and the powered-on unit with volumes mounted is (per guide 33) an opportunity not to squander with a power cut.

§ 0 4 · GETTING IT OUT

Acquisition options: live, disks-out, or hybrid

- **Live collection from the running unit** (the usual first choice where the box is healthy and credentials exist): forensic collection of shares over the network or attached storage, metadata preserved, hashed and manifested; snapshot states mounted and collected; appliance configuration, user list and logs exported; the whole exercise logged per protocol. Business disruption: minimal; the unit keeps serving.
- **Disks-out imaging with reconstruction** where the unit is contested, failing, encrypted-with-keys-available-offline, or must be seized: documented shutdown; each disk photographed in its bay, labelled, removed in order; every member imaged individually; the array reconstructed virtually in the laboratory and mounted read-only. The strongest custody posture; the slowest route; the only route for dead or dismantled boxes.
- **Hybrid in practice:** live collection of the current state plus seizure or imaging afterwards where the matter warrants both; or live collection now with the schedules suspended, and disks-out reserved as the escalation if deletion is later suspected.
- **Choose by the guide 32 logic:** contested box, deletion suspected, attribution on the appliance itself in issue → the fuller method; cooperative custodian, documentary content the target → live collection with the history layer preserved. The protocol records which and why.

§ 0 5 · WHAT THE BOX REMEMBERS

What the appliance records: accounts, logs, snapshots, recycle folders

- **Accounts and permissions:** the NAS's own users and groups, per-share permissions, and admin roles: the map of possibility, exported as an exhibit; plus the appliance's record of joined domains where it authenticates against company directories.
- **Connection and access logs:** logons to the unit (interface and file protocols) with accounts, source addresses and times; file-access logging per share where the owner enabled it (often not: establish the configuration first, per guide 43's audit-ceiling discipline); and app-specific logs (sync, backup, surveillance) with their own retentions.
- **Snapshots and versions:** appliance snapshot series (Btrfs/ZFS-based on the major vendors) holding point-in-time share states: the history layer, differenced for change chronologies exactly as on servers, and pruned on schedules the preservation email must stop.
- **Network recycle bins:** per-share deleted-file folders (with deleter and deletion time in many configurations), emptied manually or on timers: the first stop for "destroyed" documents, before anyone reaches for reconstruction.
- **Job histories:** backup tasks (to USB, to cloud, to a second NAS), replication jobs and sync sessions, each logged with times and outcomes: simultaneously evidence of where else the data went and a chronology of the estate's habits, including the job that was switched off the week the dispute began.

§ 0 6 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: never examine the appliance in isolation. A NAS sits at the centre of a small ecosystem, and its evidence usually exists in several of these locations at once: the physical unit and its member disks; the office computers running sync clients (holding mirrored folders and their own guide 41/42 artefacts); mobile apps (vendor file and photo apps with cached content and access records); the vendor's cloud relay and any subscribed cloud backup (QuickConnect/C2 and equivalents, with their own account records); USB backup drives rotated in a drawer; a replication partner unit at another site or home; the router and network infrastructure (remote-access logs, port-forwarding history); the vendor account controlling the relay (an identity layer with its own access trail); and counterpart devices of every user who mapped a share. When the primary source fails: the box is missing, wiped, encrypted without keys, or the array is dead: these paths are the recovery plan, and the preservation notice should have named them from day one.

EVIDENCE	NAS UNIT	CLOUD RELAY / BACKUP	USB / REPLICA BACKUP	LOGS	COUNTERPART DEVICES	DELETED / RECOVERABLE
Files (shares)	Y	Often	Y (job-dependent)	Access logs if enabled	Sync-client mirrors: possibly	Recycle bin, snapshots: varies
Deletion events	Recycle metadata, snapshots	Sometimes (versioned cloud)	Bracketed by generations	If file auditing on	Client-side traces: possibly	Varies with schedules
User activity	Y (connection logs)	Relay account history	n/a	Y	Endpoint artefacts: Y	Log rotation limits
Remote access	Y (sessions, sources)	Y (relay logs)	n/a	Router/VPN: sometimes	Accessing device: Y	Varies
CCTV footage	Y (short retention)	Sometimes (cloud copy)	Sometimes	App logs	Viewing apps: caches	Overwrite: days to weeks

Fallback strategy in one line: if the box cannot speak, work outward: sync-client mirrors and endpoint artefacts first (fast, local, guide 41/42 methods), then USB and replica backups (whole-estate states), then the vendor cloud layer (account-controlled, preserve early), with the router and counterpart devices corroborating access throughout.

§ 0 7 · WHOSE HAND

Attribution on a shared box

- **The four links again:** file event → NAS account → connecting endpoint → person (guide 43's chain, unchanged). The appliance's connection logs supply account and source address; the endpoint's own artefacts (mapped drives, LNK files, sync-client records) put a session behind the address; the human layer argues from credentials and pattern.
- **Small-office realities bite harder:** shared logins ("office"/"scans"), the admin password on a sticky note, and guest access wide open are the norm: the map-of-possibility export often shows everyone could do everything, which reframes cases exactly as guide 43's Example 3 did.
- **Remote access widens the pool:** vendor relays and forwarded ports mean the connector may be anywhere; relay-account history, router logs and the accessing device's artefacts are the triangulation: and "someone hacked the NAS" becomes a testable hypothesis with those sources preserved.
- **The appliance's clock is evidence about itself:** NAS time settings drift and get changed; the examiner establishes clock state against reference time (and logs any change events) before a single timestamp is argued: the series' recurring clock discipline, in a box that nobody ever checked.

§ 0 8 · IN THE WILD

Worked examples

EXAMPLE 1 · THE RECYCLE BIN NOBODY KNEW EXISTED

A partnership split turned on project files "wiped by the defendant" from the office QNAP. The claimant's IT support had searched the shares and found nothing; destruction was pleaded with confidence. The laboratory's first hour found the per-share network recycle bin, enabled at setup and never emptied: the entire deleted tree, with deletion timestamps and the deleting account, plus snapshots bracketing the event to a Sunday evening. The account was the shared "office" login; the appliance's connection log gave the source address; and the defendant's home router allocation, disclosed after a targeted request, matched. The destruction claim became a restoration exercise and an attribution finding: two layers of the appliance's own housekeeping, unread by anyone until the right question was asked of the box.

EXAMPLE 2 · THE DISKS IN THE WRONG ORDER

Before instructing anyone, a claimant's director "secured the evidence" by pulling the four disks from a failed Synology and posting them in one padded envelope. No labels, no slot record, one disk audibly damaged in transit. The laboratory imaged each disk sector by sector (the damaged member recovering partially over three days), identified array order from on-disk metadata, and reconstructed the volume virtually: recovering the estate, minus what the damaged regions took. The expert report had to devote a section to the handling: the other side ran a contamination argument that a documented, examiner-led removal would never have allowed. The evidence survived; a week of laboratory time and a chunk of its weight were spent on an envelope.

EXAMPLE 3 · THE BOX WAS GONE; THE ECOSYSTEM WAS NOT

In a family company dispute, the NAS itself vanished the weekend before an inspection order: "stolen", per the respondent. The source-architecture map recovered the position without it: the office PCs' sync clients held current mirrors of the working shares (collected per guide 41, timestamps intact); a rotating USB backup drive in a desk drawer held month-end states going back two years; the vendor cloud-relay account: preserved by a same-day request: recorded remote logins to the unit at 23:10 the night before the "theft", from a residential address; and the router's port-forwarding history corroborated. The court granted adverse-inference directions on the disappearance and the case proceeded on the mirrors and backups: the appliance was lost, its evidence essentially was not, because the estate had more than one copy of almost everything.

§ 0 9 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Pulling disks:** Example 2, weekly, across the profession; the single instruction to give every client today is "touch nothing".
- **Powering off the healthy unit** before live opportunities (mounted encrypted volumes, running logs) are assessed: guide 33's calculus, ignored at the appliance.
- **No admin credential hunt** until the examiner is standing at a login screen.
- **Recycle bins and snapshots unchecked** before destruction is pleaded: Example 1's near-miss.
- **Schedules left running:** pruning, emptying, rotating and overwriting through the correspondence phase.
- **The ecosystem ignored:** sync mirrors, USB rotations, replicas and the vendor cloud unpreserved: and the recovery plan of Example 3 forfeited.
- **CCTV retention missed** where the box records cameras: footage overwritten in days while letters are exchanged.
- **Attribution from the NAS account alone,** on boxes where the account is the whole office.

Technical limitations

- **Vendor variance is real:** logging depth, snapshot capability, recycle behaviour and export mechanisms differ by vendor, model and firmware; the examiner establishes this unit's actual capabilities before anyone promises findings.
- **File-access auditing is usually off** in small deployments; actuality is then endpoint-built, per the audit-ceiling discipline.
- **Damaged members limit reconstruction:** parity tolerates defined failures; beyond them, recovery is partial and the report quantifies what the dead regions took.
- **Encrypted volumes without keys defeat content examination;** the ecosystem paths (§6) become the estate.
- **Appliance logs are short-horizon by default:** weeks, not years; the preservation email and early export define the reachable past.

§ 10 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- Where is the unit, what state is it in, and who has touched it since the dispute arose? (Then: nobody touches it again.)
- Who holds the admin credential and any volume-encryption keys: owner, IT support, the installer, a password manager?
- Map the ecosystem with me: sync clients on which PCs, USB backup drives, a second unit anywhere, vendor cloud services, phone apps, CCTV?

Ask your opponent

- Please preserve the NAS unit and all member disks in their current state and slots, making no removals, rebuilds, resets or firmware changes, and suspend all snapshot pruning, recycle-bin emptying, log rotation and backup overwriting pending collection.
- Please identify and preserve all associated sources: synchronised folders on any computer, USB or replica backups, vendor cloud or relay accounts, and provide the appliance's user list, permission structure and logging configuration.
- Please confirm the admin credentials and any encryption keys will be made available for examination under the agreed protocol.

Ask your eDiscovery / forensic provider

- Live collection, disks-out, or hybrid for this unit and matter: and why?
- What will you export from the appliance itself (configuration, users, logs, snapshot inventory, job histories) as exhibits?
- If the box is dead or missing, what is the ecosystem plan and its expected yield?

SUGGESTED WORDING · CLIENT HOLDING INSTRUCTION (SEND TODAY)

> "Until our examiner attends: (1) do not remove, reorder or reinsert any disks, and do not press rebuild, reset or repair options under any circumstances; (2) leave the unit in its current power state and photograph it, its display and its cabling as found; (3) suspend all automatic deletion: snapshot pruning, recycle-bin schedules, log rotation and backup-job overwrites; (4) locate the administrator credentials and any encryption keys and hold them for the examiner; and (5) preserve untouched all connected copies of its data: computers with synchronised folders, USB backup drives, any second unit, and the [vendor] cloud account. Nothing about this unit can be safely improvised; these steps keep every option open."

§ 11 · QUICK CONTROL

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

The NAS evidence checklist

- ☐ Unit preserved as found: no disk-pulling, no rebuilds, power state photographed
- ☐ Holding instruction issued day one; schedules suspended; confirmations filed
- ☐ Admin credentials and encryption keys hunted immediately across owner, IT, installer, managers
- ☐ Acquisition route chosen by protocol: live, disks-out with documented removal, or hybrid
- ☐ Appliance exhibits exported: configuration, users and permissions, logging setup, snapshot inventory, job histories
- ☐ Recycle bins and snapshots examined before any destruction allegation is pleaded
- ☐ Source architecture mapped and preserved: sync mirrors, USB and replica backups, vendor cloud, phone apps, router logs, CCTV
- ☐ Clock state established before timestamps are argued
- ☐ Attribution built on four links, with endpoint correlation; shared-login realities faced in the report
- ☐ All layers delivered under one custody record, limitations (audit ceiling, log horizons, damaged members) stated

Red flags

- Disks in an envelope.
- "We reset it to check it still worked."
- No admin password and no hunt started.
- Destruction pleaded with recycle bins and snapshots unexamined.
- A unit that "was stolen" the week of an inspection order, with the ecosystem unpreserved.
- Timestamps argued from a box whose clock nobody verified.
- Vendor cloud and sync copies outside the preservation notice.

When to involve a digital forensic expert

Before anyone touches the box: the holding instruction and credential hunt are day-one, and disk-pulling prevention alone justifies the call. For acquisition, always: RAID handling, live-versus-disks-out judgment and appliance exports are laboratory work. For the ecosystem, early: the §6 map turns a single point of failure into a resilient estate, but only if its members are preserved before they churn. And in dispute, both ways: the CPR Part 35 report that reads the appliance's own records properly (Example 1), or the review that prices an opponent's improvised handling (Example 2) and disappearing hardware (Example 3) at their true evidential cost.

§ 12 · COMMON QUESTIONS

Frequently asked questions

One of the disks has failed. Is the data gone?

Usually not: failure-tolerant RAID modes are designed to survive defined disk losses, and even the failed member often images partially in the laboratory. The dangerous moment is not the failure but the response: rebuilds and swaps on suspect hardware can overwrite recoverable material. Power down on advice, touch nothing, and let imaging-then-virtual-reconstruction do the work: the route that preserves both the array and every option.

The NAS is password-protected and the person who set it up has left. Now what?

Hunt first: installers, IT suppliers, password managers, documentation, and the vendor account (which sometimes enables recovery routes on managed units). In parallel, assess the ecosystem: sync mirrors and backups frequently contain the estate without the appliance's cooperation. Laboratory options on the unit itself depend on model and configuration (unencrypted volumes on extracted disks are readable regardless of the interface password; encrypted volumes need their keys): an examiner will tell you which case you have within a day of seeing the model.

Files were deleted from the NAS months ago. Recoverable?

Check, in order: the share's network recycle bin (deleted files often sit there for months); snapshot series (states bracketing the deletion, if pruning has not eaten them: hence the day-one suspension); backup generations (USB rotations and replicas reach furthest); and cloud-versioned copies where a sync or backup service was running. Classic carving inside the array is a last resort with modest odds on modern configurations. The honest answer is schedule-dependent: which is why this guide keeps sending the preservation email today.

Can we prove who deleted them?

Often to the account and endpoint, per the four links: recycle metadata and file-access logs (where enabled) name the NAS account and time; connection logs give the source address; the endpoint's own artefacts and, for remote access, relay and router records complete the triangulation. On boxes run on shared logins, the account link names a pool and the endpoint layer does the real work: the report should say exactly that, because overclaiming here is where NAS cases go to die in cross-examination.

The unit also records our CCTV. Anything special to do?

Move fastest on this of everything: surveillance retention is typically days to a few weeks and overwrite is continuous. Today: stop or reduce recording if the footage matters more than new coverage (a business decision to make explicitly), export the relevant date ranges through the surveillance app with times and camera identifiers, and preserve the app's logs. The dedicated CCTV guide later in this series covers format and timestamp handling; the NAS-specific point is simply that the deadline is the box's own timer.

Is a home NAS different from an office one?

Legally more than technically: the same vendors, arrays and artefacts, but personal ownership engages the consent, proportionality and privacy frameworks of this series' personal-device guides, and household sharing complicates attribution further. Practically, home units are more often the replication partner or backup target of an office box (Example 3's second copy), which makes them disclosure-relevant through the ecosystem even when nobody thought of them as company systems: one more reason the §6 map belongs in every preservation notice.

§ 13 · REFERENCE

Glossary

Array metadata
On-disk configuration data enabling laboratory reconstruction of disordered members.

Degraded array
An array running after a member failure; recoverable, fragile, not to be rebuilt casually.

Member disk
One drive of a RAID set; individually unreadable stripes, collectively the volume.

Network recycle bin
Per-share deleted-file folder on the appliance, often with deleter and time recorded.

Parity
Recovery information spread across members, letting arrays survive defined failures.

Relay / vendor cloud
Manufacturer service (e.g. QuickConnect-type) enabling remote access and cloud backup; its account holds its own logs.

Replication partner
A second unit receiving copies on schedule; the off-box history layer.

Snapshot series
Appliance point-in-time share states; the history layer, pruned on schedule.

Sync client
Desktop/mobile software mirroring NAS folders to endpoints; the ecosystem's fastest fallback.

Virtual reconstruction
Assembling imaged members into a mounted read-only array in the laboratory.

Sources and authoritative references

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

- cflab.uk, digital forensics services (NAS and RAID acquisition and reconstruction, deleted data recovery, appliance log analysis, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 02 · Preservation and Phase 03 · Collection (ecosystem preservation and appliance collection at disclosure scale): 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
- NPCC / College of Policing digital evidence guidance: college.police.uk, digital devices guidance · ISO/IEC 27037:2012: iso.org, 27037
- CPR Part 31 / PD 57AD (preservation duties) and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35
- ICO, UK GDPR guidance (including CCTV/surveillance): ico.org.uk

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

NAS work spans the laboratory's bench and the field: same-day holding instructions and credential hunts, live collection to protocol from healthy units, documented disks-out seizure with virtual reconstruction for contested and failed arrays (damaged members included), and the appliance exhibit set: configuration, users, logs, snapshots, job histories: exported before schedules eat it. We map and preserve the ecosystem (sync mirrors, backups, replicas, vendor cloud, CCTV) so the estate survives even when the box does not, and we report under CPR Part 35 with the four-link attribution and stated limitations this series requires. Through **e-discovery.uk**, NAS collections flow into disclosure-scale processing beside every other source. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; if a unit is at risk today, call before anyone touches a disk.

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