

A CCTV disclosure log is the building's record of who received footage, when it was disclosed, why it was needed and what happened to the exported copy. It helps a management team answer questions consistently, demonstrate accountability and spot poor practices before they become incidents of their own.

For a residential or mixed-use building, the log should sit within a wider CCTV governance process. A spreadsheet alone cannot make an unnecessary camera appropriate, fix an unclear purpose or protect an exported clip saved to an open shared folder. Start with the security purpose, decide who may authorise disclosure, and make sure every export has a controlled destination and deletion plan.

This guide is for property managers, building operators and owners' or residents' associations in the UK. It is operational guidance, not legal advice. Check current Information Commissioner's Office (ICO) guidance and obtain advice where a request or disclosure is complex.

## Start with the reason for disclosure

Before anyone searches a recording, ask: **What security question does this camera answer?** <https://realtytimes.com/new-headlines/cctv-in-elevators-and-common-areas-property-manager-responsibilities>

Then ask the same about the request: **What is the reason for disclosure?** A clear answer helps establish whether footage is relevant, whether a search is justified and how much material is actually needed.

Common examples include investigating a reported assault, theft, damage to property, vehicle collision or a specific safety incident. A request might come from a resident, an insurer, the police, a solicitor or a person exercising their data protection rights. The fact that somebody has asked for footage does not automatically mean the whole recording should be shared.

Here's what kills me: record the reason in neutral, factual language. "Resident asked for footage" is not enough. A better entry might say: "Footage from the east entrance requested to review a reported fall between 18:10 and 18:25 on 14 May." Avoid speculative commentary or unnecessary personal details.

## Agree who owns and governs CCTV decisions

Write down who is responsible for the CCTV system and who can make decisions about access and disclosure. In many buildings, the relevant organisation may be an owners' association, management company or other operator. The correct position depends on who determines the purposes and means of processing. Do not assume that the maintenance contractor, managing agent or camera installer is automatically the decision-maker.

Set out responsibilities in a policy or procedure. For example:

- **System owner or controller:** approves the purpose, camera coverage, retention settings and disclosure policy.
- **Authorised operator:** searches footage for an approved purpose and records the search and export.
- **Approver:** reviews higher-risk disclosures, such as releases to third parties or footage showing sensitive circumstances.
- **Installer or service provider:** maintains equipment under documented instructions and does not browse footage without authorisation.

Limit access to people who need it for their role. Curiosity is not a reason to view CCTV. Keep a record of authorised users, review access periodically and remove permissions promptly when someone changes role or

leaves.

## Check camera placement and field of view

A disclosure log cannot compensate for cameras that collect more information than necessary. Review each camera's purpose and field of view. Does it cover the entrance, lift lobby, mailroom or garage area relevant to a documented security need? Does it also capture private windows, neighbouring property, staff break areas or public space that is not needed for that purpose?

Use physical positioning, privacy masking and camera settings to limit unnecessary capture. Recheck views after building works, landscaping changes or equipment adjustments. Keep a simple camera register recording each device's location, purpose, view, owner and retention setting. If a camera has no defensible purpose, consider whether it should be repositioned, switched off or removed. "Just in case" is not a useful purpose statement.

## What to put in the disclosure log

Use a restricted-access log with one entry for each request and each resulting disclosure. A request that is refused or cannot be fulfilled should also be recorded. Use a unique reference number so the log can be discussed without repeatedly copying names into emails or reports.

Log field What to record Reference number A unique ID for the request and any related export. Request received Date received, requester's organisation or role, and a contact route stored securely. Reason for disclosure The stated purpose and the incident or lawful basis being considered. Footage searched Camera or area, date and time range, and who conducted the search. Decision and approver Whether footage was disclosed, limited, refused or referred for advice, and who authorised the decision. Recipient and date Record recipient and date: identify the recipient, the date and time sent or handed over, and the delivery method. Export details File or export reference, format, duration, redactions applied and any relevant integrity checks. Export retention plan Where the exported clip is stored, who can open it, the deletion or review date, and who is responsible for deletion.

Keep the log factual and proportionate. Avoid making it a second copy of the footage or a place for informal opinions. If sensitive details are needed to handle the request, store them in an access-controlled case file and refer to that file by reference number.

## Use a consistent request and decision process

1. **Register the request.** Note when it arrived, who made it, what incident or time period it relates to and how the requester can be contacted.
2. **Clarify the scope.** Ask for a specific date, time, location and reason where these are missing. Do not search every camera or a full day of footage if a narrower search will answer the question.
3. **Check authority and necessity.** Confirm the requester's identity and role where appropriate. Consider whether disclosure is permitted and necessary, and whether the request should be handled as a data protection rights request or another type of request.
4. **Search and document.** An authorised operator searches only the relevant cameras and time window. Record what was checked, including if no footage was found or the system had overwritten it.
5. **Review before release.** Check who else appears, whether the clip includes more information than needed and whether redaction or a narrower extract is appropriate.
6. **Approve and transfer securely.** Record the decision, recipient and date, chosen transfer method and any conditions communicated to the recipient.

7. **Close the record.** Confirm where the export was stored, who can access it and when it must be deleted or reviewed. Record completion of deletion when it occurs.

Disclosure decisions can depend on the circumstances and applicable law. For example, a person asking for their own personal data may have rights that need to be assessed, while footage may also show other people. A police request should be verified and handled through an appropriate secure channel. Escalate uncertain, disputed or high-risk cases rather than improvising.

## Redact thoughtfully, not just faces and number plates

Before sending footage, review the whole clip and the audio, if audio recording is enabled. Audio should not be collected or disclosed casually; first confirm that its use is necessary, lawful and covered by the building's policy.

Redaction checks should go beyond faces and number plates. Look for:

- names, access credentials, delivery labels and information visible on screens or documents;
- children and other people who are not relevant to the request;
- door codes, keypad entries, security procedures or restricted-area details;
- reflections, glass surfaces and background views that reveal additional people or private spaces;
- audio that captures unrelated conversations or sensitive information; and
- metadata, file names or accompanying notes that expose more information than intended.

Redaction must genuinely obscure the information in the exported file. Let me tell you about a situation I encountered wished they had known this beforehand.. A black box that can be removed, a blur that is too weak or an edited preview with the original still attached is not sufficient. Verify the final export before release and retain a record of what was redacted and why.



## Control the export: destination, access and deletion

Always ask: **Where will the exported clip end up, and who can open it?** Raw clips emailed around, downloaded to personal devices or dropped into a broadly shared folder are difficult to control. Use an approved encrypted transfer method or a restricted case-management location. Verify the recipient and avoid sending access links to group mailboxes unless each person's access is authorised.

Set an export retention plan before sending the clip. Identify the storage location, named or role-based access, the retention period, the deletion date and the person responsible for checking deletion. If a recipient needs to retain footage for a legal or insurance process, record the stated need and any agreed review point. Do not promise that a recipient will delete a copy unless the terms and process support that expectation.

Keep the original recording and exported copy distinct in your records. The building's routine CCTV retention period may be shorter than the retention needed for a specific incident, but any decision to preserve footage should be limited to the relevant material and documented. At the end of the approved period, delete the export securely and record the date. A shared folder with no deletion date is not a retention plan.. Pretty simple.

## **Set routine retention and deletion rules**

Choose retention periods based on the security purpose, the time needed to identify and report incidents, and the system's practical operation. Avoid keeping footage indefinitely because storage is available. Explain the normal retention period in the CCTV policy and privacy information, then configure the system to delete or overwrite routinely.



Document exceptions. If an incident requires footage to be held beyond the normal cycle, record the reason, the specific cameras and time range, who approved the hold, where the copy is stored and when it will be reviewed. Release the hold and delete the material when the purpose ends, unless another documented obligation applies.

## **Test the process and keep the log secure**

Limit access to the log because it can reveal incidents, identities and investigative activity. Store it separately from general building records, apply appropriate permissions and keep an audit trail where possible. Decide how long log entries themselves should be kept, based on accountability and operational needs, and include that period in the records schedule.

Review a sample of entries at regular intervals. Check that the reason for disclosure is specific, that the recipient and date are recorded, that exports have an owner and deletion date, and that access was limited to authorised people. Use findings to improve training, camera positioning and policy. If a pattern of requests suggests a camera is aimed too broadly, revisit its field of view rather than treating every disclosure as an isolated event.

## Common mistake: no prices listed in the scraped article

If you are comparing CCTV products or services, a scraped article may contain no prices. Do not fill the gap with invented figures or imply that a camera, storage plan or redaction tool has a standard cost. Pricing varies by system, building, installation, storage and support requirements. Request current quotes from suppliers and compare the full operating costs, including secure exports, access controls, maintenance and deletion capability.

For a disclosure log, the important question is not simply what the system costs. Ask whether it supports controlled searches, reliable exports, appropriate access restrictions and a practical way to record retention and deletion. A low-cost setup that encourages uncontrolled copying may create more work and risk than it saves.

## Make the log part of the building's CCTV governance

A useful disclosure log connects the request to the decision, the recipient and the final disposition of the footage. Pair it with a camera register, access list, retention schedule and written procedure. Keep the process proportionate, train staff not to browse footage out of curiosity, and review decisions when the building or its security needs change.

With those controls in place, the log becomes more than a record of files sent. It shows that the building considered why footage was needed, limited what it captured and shared, and took responsibility for where each export went and how long it remained accessible.

## Share this guide

- [Share on Facebook](#)
- [Share on X \(Twitter\)](#)

*Replace the example.com address with the published URL of this article before using the share links.*