A request for CCTV footage can sound straightforward: “Something happened in the building. Can you check the cameras?” But if the person will not provide even an approximate date or time, that request may cover hours—or days—of recordings across several cameras. It can also capture residents, visitors, staff and passers-by who have nothing to do with the incident.

The practical answer is to pause and ask for enough detail to locate the relevant footage. A **request must identify the incident** with a **narrow date and time**, or at least a workable time window and location. If the requester cannot provide those details, do not respond by searching broadly or exporting everything that might be relevant. Explain what information is needed, preserve footage only where there is a specific reason to do so, and follow the building’s CCTV policy and applicable data protection requirements.

This is an operational guide for property teams and building managers. It is not a substitute for advice from your data protection lead or solicitor, particularly where a police request, legal claim or formal data subject request is involved.

Why a request with no time is a problem

“Please send me everything from the lobby last week” is not a focused incident request. The footage may show many people going about ordinary business, and reviewing it could require staff to watch a large volume of recordings without a clear purpose. The longer and wider the search, the greater the risk of unnecessary viewing, disclosure or retention.

Data minimisation is a useful reality check: collect, view and disclose only what is necessary for a defined purpose. Ask: **What security question does this camera answer?** If the requester cannot explain what happened, roughly when it happened or where it took place, it is difficult to identify what footage is necessary to answer that question.

That does not mean every request without an exact timestamp should be rejected. People may remember only that an incident happened “after school”, “around lunchtime” or “on Saturday evening”. Ask for the best available estimate and narrow the search collaboratively. The aim is a usable window, not impossible precision.

What details to request before searching

Use a standard intake checklist so that staff ask consistent questions and record the answers. Ask the person to provide:

- **The incident:** What happened, and what are they trying to establish?
- **The date:** The exact date, or the narrowest date range they can give.
- **The time:** An exact time or a reasonable estimate, including how certain they are. Ask for the narrowest practical window.
- **The location:** The lobby, lift, entrance, car park, mailroom or another specific area.
- **People or items involved:** A description that helps locate the event, without asking for irrelevant personal details.
- **The purpose of the request:** For example, reporting damage, locating a parcel or providing information about a safety incident.
- **Urgency and deadlines:** Whether there is an immediate safety concern, a police investigation or a formal legal deadline.

If someone cannot supply an exact time, help them work it out. Ask when they first noticed the problem, when they last saw the item, when they arrived or left, or whether a receipt, message or access record can narrow the window. Make clear that these details are used to locate relevant footage, not to investigate unrelated activity.

Set a reasonable boundary

You can say: "We can check for footage once we have enough detail to identify the incident. Please give us the date, the area and your best estimate of the time. Without that, we may have to review a large amount of footage showing other people, so we cannot begin a broad search."

If the requester still will not narrow the request, explain the next step under your policy. Depending on the circumstances, that might mean asking them to clarify, referring the request to the building's privacy contact, or explaining that the request cannot be actioned as submitted. Avoid promising that footage exists or that it will be released.

Do not turn uncertainty into a fishing expedition

An open-ended search for "anything useful" is a fishing expedition, not a sound review process. It encourages staff to watch recordings without a defined incident, increases the chance of seeing unrelated private activity, and can make it harder to justify why footage was accessed.

Keep searches proportionate. Start with the camera most likely to cover the reported location and the narrowest credible time window. Expand only if there is a recorded reason—for example, the incident may have moved from the entrance to the lift lobby. Do not browse other cameras simply because they are available.

Be especially careful with requests that appear to be about monitoring a neighbour, tracking someone's routine, checking who visits another resident, or resolving a personal dispute. A CCTV system should not become a convenient way to satisfy curiosity. Refer doubtful requests to the person or body responsible for CCTV governance before anyone views footage.

Preserve footage only when there is a specific reason

Many systems overwrite recordings automatically after a set retention period. If the incident is specific and the footage may be needed for a legitimate review, a time-limited preservation step may be appropriate. Record why it was preserved, which camera and period are involved, who authorised realtytimes it and when it will be reviewed again.

Do not respond to a vague request by putting large amounts of footage on indefinite hold. A preservation step is not a reason to abandon routine deletion. If no usable details arrive, follow the normal retention schedule unless a separate legal, safety or law-enforcement reason requires otherwise. Seek advice where the circumstances are unclear.

Retention periods and routine deletion

Set a retention period that reflects the building's actual security purpose, technical capacity and risk assessment. There is no single retention period that suits every property. A busy mixed-use building with an identified incident process may have different needs from a small residential block, but "keep it just in case" is not a defensible retention policy.

Document how long footage is kept, why that period is necessary, who can authorise an extension and how deletion is checked. Routine deletion should happen automatically where possible, with a clear process for recordings that have been validly preserved. When the reason for a hold ends, release it back into the normal deletion cycle.

Review the schedule periodically. Ask whether the retention period is still needed, whether footage can be found quickly enough to support incident reporting, and whether staff are extending holds informally. A written policy is only useful if the system and the onsite practice match it.

Who owns CCTV decisions?

In a managed building, cameras may have been installed by the freeholder, an owners' association, a management company or another organisation. The organisation that determines why and how the system is used generally has responsibility for its governance. Confirm this rather than assuming that the onsite manager, concierge or security contractor can make every decision.

Write down who is responsible for:

- approving the purpose, camera locations and field of view;
- setting access permissions and authorising footage reviews;
- handling requests from residents, visitors, insurers, solicitors and police;
- approving exports, disclosures, redactions and preservation holds; and
- maintaining the retention schedule, access log and deletion process.

Board members and property staff should not casually watch clips or ask an operator to "have a look" without a defined reason. Access should be role-based and logged. Where a request may involve another person's personal data, or the requester wants a copy, involve the designated privacy contact and follow the formal process. A request to view footage is not automatically a right to receive an unredacted copy.

Camera placement and field of view matter

Good request handling begins before an incident. Each camera should have a defined security purpose and an appropriate field of view. Check whether it captures only the area needed—for example, an entrance or lift doors—or also records private spaces, neighbouring property, windows, staff work areas or public areas beyond what is justified.

Use camera positioning, privacy masking and system settings to reduce unnecessary capture. Avoid installing cameras "just in case". If a camera's purpose cannot be explained, review whether it is needed at all. Changes to angle, zoom or coverage should be approved and recorded, not made informally to follow a particular person.

When assessing a request, the camera's field of view can help determine whether it is relevant. A camera that does not cover the reported location should not be searched merely because it is easy to access. Keep a simple camera map and a record of each camera's purpose so staff can identify the likely source without viewing unrelated footage.

Review, export and disclosure safely

If a focused search finds relevant footage, limit review to the necessary period and people. Keep a note of the reviewer, date, camera, time range, reason for access and outcome. If the recording is exported, record the file name or reference, who approved it, where it is stored, who can open it and when it will be deleted.

Do not email raw clips around or place them in a broadly shared folder. Use an approved, access-controlled location and a secure transfer method. Set an expiry date for temporary links or copies, and restrict access to people who need it for the stated purpose.

Redaction is not just a matter of blurring faces and number plates. Consider whether a clip reveals:

- children, visitors, staff or other residents who are not relevant to the incident;
- door-entry codes, keys, access cards or security procedures;
- unit numbers, delivery labels, computer screens or private documents;
- audio or conversations, if audio has been captured;
- personal routines, health-related information or other sensitive context; and
- camera positions or blind spots that could create a security risk.

Redact only as needed and preserve the original securely if policy or legal advice requires it. Do not edit a clip in a way that changes the meaning of the event. If the footage cannot be shared safely, explain the available alternatives through the proper process rather than sending an unredacted file.

A practical response workflow

1. **Acknowledge the request.** Record who made it, when it arrived and the general purpose.
2. **Ask for missing details.** Request the incident, a narrow date and time, the location and the best estimate available.
3. **Check authority and urgency.** Follow the building's policy and refer formal, sensitive or unclear requests to the responsible privacy contact.
4. **Decide whether to preserve.** If there is a specific, credible incident and footage may be overwritten, document a limited hold and its review date.
5. **Search proportionately.** Use the relevant camera and time window first; record any justified expansion.
6. **Control access and any export.** Log who viewed or received footage, where it is held, who can open it and the deletion date.
7. **Close the request.** Record the outcome, notify the requester as appropriate and remove preserved copies when the reason ends.

Sample reply when the requester will not give a time

"Thank you for contacting us. To check the relevant CCTV, please tell us what incident you are reporting, the area involved, the date and your best estimate of the time. A narrow time window helps us avoid reviewing footage of other residents, visitors and staff. If you do not know the exact time, please provide an approximate window and explain what may help us narrow it. We cannot carry out an open-ended search or provide footage without reviewing the request under the building's CCTV and privacy procedures."

If the person gives a broad range, ask one follow-up question at a time. For example: "Could you narrow 'Tuesday afternoon' to before or after 3 pm?" Keep the exchange factual and courteous. Do not suggest that the building will search every camera until something is found.

Keep the process transparent

Tell residents and other users what CCTV is for, where cameras operate, how long recordings are normally kept and how to make a request. A clear sign is useful, but it does not replace a proper policy or an explanation of who handles requests. Keep the policy aligned with actual camera coverage, system permissions and retention settings.

Facebook share: Share this guidance with your building team or residents' committee using the Facebook share option.

X (Twitter) share: Share a concise reminder on X (Twitter): "CCTV requests need an incident, location and narrow date and time. Avoid fishing expeditions; log access, control exports and delete footage on schedule."

Final checklist

- Can the requester identify the incident and give a narrow date and time?
- Is the camera relevant to the location and purpose?

- Is any preservation limited, justified and due for review?
- Are access, viewing and any disclosure logged?
- Do you know where exported clips end up and who can open them?
- Have you considered redaction beyond faces and plates?
- Is there a clear deletion date for every retained copy?

When a requester will not give a time, the safest response is not to guess, browse widely or send a clip. Ask for enough detail to identify the incident, keep any search proportionate and make sure CCTV decisions are governed, recorded and time-limited.