

A contractor asks to see CCTV after a leak, lift fault, damaged door or reported incident. The request may sound straightforward: “Can you send me the footage?” But a building’s camera system can capture residents, visitors, staff, vehicle registrations and private activities unrelated to the job. Giving someone a login or emailing a clip can create a new privacy and security problem while you are trying to solve the original one.

For most routine building incidents, the safest starting point is **supervised viewing CCTV**: an authorised building representative reviews the relevant footage, then arranges a controlled viewing if the contractor genuinely needs to see it. Share only the necessary information, for a defined purpose and period. Avoid granting broad system access or handing over a downloadable copy by default.

This guide sets out a practical approach for property managers, owners’ associations, onsite teams and contractors. It is operational guidance, not a substitute for advice on your organisation’s legal duties. Check your CCTV policy, contracts and applicable data-protection requirements before disclosing footage.

Start with the security question

Before you approve any access, ask: **What security question does this camera answer?** The answer should be specific. For example: “Did the contractor leave a trolley in the fire-door route between 10:00 and 10:30?” is more useful than “They want to look around the cameras.”

Then establish whether [realtytimes.com](https://www.realtytimes.com) CCTV is actually needed. Can a work order, access-control log, incident report, photograph of the affected area or direct inspection answer the question with less exposure of other people’s information? Data minimisation means using the least intrusive information that will do the job—not treating recorded footage as a convenient general-purpose resource.

Clarify who is asking, why and what they need

Do not treat “the contractor” as a single, self-explanatory identity. Confirm the requester’s name, employer, role and authority to make the request. Verify the request through a known contact at the contractor’s organisation, rather than relying only on an unexpected email or phone call.

Ask for the purpose and scope in writing. A useful request states:

- the incident, work order or safety issue being investigated;
- the date, time range and specific camera or location involved;
- why CCTV is needed, and why another source will not be enough;
- the names and roles of the people who need to view it;
- whether the contractor is seeking a viewing, a still image or a copy; and
- how any information received will be secured, used and deleted.

If the request is vague, concerns a whole day or asks for access to multiple cameras without a clear reason, pause and ask for a narrower request. A contractor’s interest in an incident does not, by itself, authorise access to every person captured in the footage.

Keep CCTV decisions with the responsible organisation

Agree who owns and governs CCTV decisions before an incident occurs. Depending on the building and its arrangements, responsibility may sit with the property owner, management company, owners’ association or

another designated organisation. A managing agent or onsite team may operate the system, but that does not automatically mean each member of staff can approve disclosures independently.

Document a simple approval route. It should identify who can authorise a search, who can arrange a viewing or disclosure, when a privacy lead or senior manager must be consulted, and how decisions are logged. Check the building's CCTV policy and service agreements, and seek advice where responsibilities are unclear or the request is sensitive.

Keep the decision separate from the person who is simply curious or directly involved in the incident. Staff, board members and contractors should not browse footage "just to see what happened". Every search should have a recorded purpose, an authorised requester and a defined scope.

Prefer supervised viewing over open access

Where viewing is justified, **supervised viewing CCTV** is often a safer option than supplying a copy. An authorised representative locates the relevant time window and camera, checks the material, and arranges a viewing in a controlled setting. The contractor sees only what is needed, with an authorised member of the building team present.

Supervision is not a licence to reveal unrelated footage. Pause or narrow the viewing if other residents, visitors or activities appear that are not relevant. Do not allow the contractor to photograph the monitor, record the screen on a phone, connect a personal device or navigate freely through the recorder. Make clear that viewing is for the stated purpose only.

Where possible, prepare a short, relevant segment rather than showing a continuous feed or an extended recording. If the contractor only needs to confirm that a delivery was made, they may not need to see the entire loading-bay sequence. If the issue can be resolved by giving a factual summary, that may be enough.

Use temporary access controls if access is unavoidable

Sometimes a contractor has a genuine technical need to inspect a CCTV system—for example, to diagnose a camera fault. That is different from asking to review recorded footage about an incident. Separate system maintenance from footage access, and limit the contractor's permissions to the job.

Use **temporary access controls** where the system supports them. These may include a named, individual account; read-only permissions; access to one camera or a restricted time period; a time-limited account that expires automatically; and a record of logins and actions. Have an authorised staff member present where practical, and revoke access as soon as the task ends.

Never share an administrator password, a general team login or a permanent account created for a one-off visit. Confirm beforehand whether the account can export recordings, view live feeds, change camera settings or access other locations. Disable functions the contractor does not need.



Adopt a no downloadable copy rule by default

A useful operational standard is a **no downloadable copy rule** for contractor requests unless a named decision-maker approves an exception. Once a clip leaves the CCTV system, it can be copied, forwarded, saved to an unmanaged device or retained long after the job has finished. You may lose control over who can open it and when it is deleted.

If a copy is genuinely necessary, decide exactly why a supervised viewing will not work. Check whether the footage contains information about other people and whether the disclosure can be reduced, for example by shortening the clip or obscuring irrelevant areas. Use an approved, secure transfer method—not personal email, a messaging app or an open shared folder.

Before any export, ask the question I always ask: **Where will the exported clip end up, and who can open it?** Record the authorised recipients, purpose, transfer method, access restrictions and deletion date. Confirm secure receipt. Do not assume that a contractor's general file-storage practices are suitable for CCTV evidence.

Limit what the cameras capture

Access decisions begin before a request is made. Camera placement and field of view should be set to address defined security needs, such as monitoring an entrance, protecting a parcel area or investigating access to a plant room. Cameras should not be installed “just in case”, and their views should not extend unnecessarily into homes, changing areas or neighbouring private spaces.

Review each camera's position and field of view periodically and when building layouts change. Mask areas that do not need to be recorded, adjust angles, and restrict access to cameras that capture more sensitive areas. A camera that covers a lobby entrance may not need to record an entire seating area or a resident's doorway.

This matters when a contractor requests footage: a tightly planned view is more likely to provide useful evidence without exposing unrelated people. If the camera captures more than the incident requires, narrow the time period and consider whether a controlled summary or appropriately redacted extract is possible.

Redaction is more than faces and number plates

If a disclosure is approved, consider what should be removed or obscured. Facial blur and vehicle-registration masking are obvious checks, but they are not the only ones. Use this short review list:

- residents, visitors, children and staff who are not relevant to the issue;
- door-entry keypads, access credentials or visible security procedures;
- unit numbers, name labels, post or screens that reveal personal details;
- private areas or views beyond the building boundary;
- audio, if the system records it and it is not needed; and
- timestamps, commentary or other context that could identify people unnecessarily.

Redaction must be effective: placing a removable shape over a face in an editable file is not the same as securely obscuring it. Keep the original recording protected in the CCTV system, and provide only the approved, reviewed version if a copy is authorised.

Set retention periods and delete routinely

Footage should not be retained indefinitely because it might be useful someday. Set a routine retention period that fits the building's documented purposes and applicable requirements, then configure the system to overwrite or delete recordings automatically where appropriate. Retain a specific clip longer only when there is a recorded reason, such as an active investigation, insurance matter or legal hold.

A contractor's request should not quietly turn a routine recording into a permanent archive. If footage is preserved for a defined purpose, record what is being held, who approved it, where it is stored, who can access it, and the review or deletion date. At the end of the matter, confirm whether the preserved copy must be securely deleted and document the action.

Apply the same discipline to exports, screenshots, viewing-room notes and temporary working files. A clip saved "for later" on a desktop or shared drive is still a copy that needs access control and a deletion date.

Record the decision and the disclosure

A concise CCTV access log helps the organisation show that decisions were deliberate and consistent. Record both approved and refused requests. A log might include:

Record What to note Request Requester, employer, date received, stated purpose and incident reference. Scope Camera or location, date and time range, and material reviewed. Decision Who approved or refused access, the reason and any conditions. Method Supervised viewing, restricted system access or approved secure transfer. Handling Recipients, redactions, storage location, access controls and deletion date.

Keep the log in the organisation's approved records system, not in an informal email chain. Limit access to staff who need it for governance, incident management or compliance.

Do not invent a price—or leave costs unexplained

A common mistake in scraped or copied guidance is to state "No prices listed in scraped article" as if it were useful pricing information. It is not. CCTV access is a privacy and governance decision, not a standard product with a universal price. Do not invent a fee or imply that payment automatically grants access.

If the organisation may charge for a specific service, such as technical retrieval, secure export or specialist redaction, check the governing agreement and applicable rules first. Explain any legitimate charge, who bears it and what work it covers before proceeding. A cost discussion must never replace the authorisation, minimisation and security checks.

A practical decision sequence

1. **Verify** the contractor and the authority of the person making the request.
2. **Define** the purpose, incident, camera and narrowest useful time window.
3. **Test necessity**: could a less intrusive record answer the question?
4. **Approve** access through the building's designated CCTV decision-maker.
5. **Choose the least intrusive method**, normally supervised viewing rather than a copy.
6. **Apply controls**: restrict permissions, supervise, redact where needed and prohibit onward sharing.
7. **Log the decision**, recipients, storage arrangements and deletion date.
8. **Close out**: revoke temporary access and confirm deletion of any authorised copy when no longer needed.

The safest option in brief

For a contractor who needs to understand a specific building incident, start with a narrow, documented request and an authorised internal review. If access is justified, offer **supervised viewing CCTV** with a clear purpose and no phone recording. Use **temporary access controls** only when technical access is genuinely required, and apply the **no downloadable copy rule** unless a responsible decision-maker approves a secure, limited exception.



Keep camera views purposeful, retention limited and routine deletion active. And before any footage leaves the system, be able to answer: where will it go, who can open it, and when will it be deleted?

Share this guidance

- [Share on Facebook](#)

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