

A slip-and-fall video request can arrive from an injured resident, visitor, solicitor, insurer or other representative. It may feel urgent—and the footage may seem like the clearest account of what happened. But a camera can also capture bystanders, private routines, access arrangements and unrelated incidents. Sending an entire recording, or letting someone browse a camera system, can disclose far more than the requester needs.

A safer response starts with a simple question: **What security question does this camera answer?** Then identify the relevant time and place, preserve material that may relate to a claim, and disclose only what is authorised and necessary. The exact legal position depends on your jurisdiction and the circumstances, so involve your organisation's privacy lead or legal adviser when in doubt.

Start with the incident, not the camera archive

Surveillance footage is personal data when people can be identified from it. That does not mean every request automatically entitles someone to a copy of every recording in which they appear. It does mean that requests should be handled through a consistent, documented process, with privacy, safety and applicable disclosure obligations considered together.

Begin by establishing what happened and what the requester is asking for. Collect only the details needed to locate the relevant material:

- The date and approximate time of the incident, including any uncertainty.
- The location, such as a lobby entrance, lift landing, stairwell or garage walkway.
- The person's role and, where appropriate, how they can be identified.
- The requested time range and whether the request is for viewing, a copy or preservation.
- The requester's authority if they are acting for someone else.

Ask for a narrower time window if the request is broad. "All footage from the lobby that afternoon" may capture dozens of people and unrelated activity. A more focused request might identify the period before and after the reported fall. If the exact time is unknown, work with the requester to establish a reasonable search range, then refine it using incident logs or other relevant information.

Limit to incident segment

Use the fewest cameras and the shortest time span that can reasonably show the reported event and its immediate context. This is the practical meaning of **limit to incident segment**: do not export an entire shift, a full day or every camera angle merely because it is convenient.

The relevant segment may need to include more than the moment of the fall. A short period before it may show a spill, obstruction or route through the area; a short period afterwards may show the response. The appropriate boundaries depend on the incident and the question being investigated. Record why you chose them.

Before exporting, check the camera's field of view. Does the view include an adjoining flat entrance, a reception desk, a changing area or another space where people have a stronger expectation of privacy? Is the incident visible from another camera with a narrower view? Use the least intrusive usable source. If no suitable recording exists, say so rather than searching unrelated footage without a clear purpose.

Camera placement and field of view should be reviewed as part of ongoing governance, not improvised after an incident. Cameras should address a defined security or safety need. Avoid broad views installed "just in case", and

regularly check that camera angles still serve their stated purpose. Changes to a camera's position or field of view should be authorised and documented.

Preserve for claim, then control access

Routine deletion is an important privacy safeguard. It prevents footage from accumulating indefinitely and limits the harm if an account is compromised or access is misused. But when a credible incident or claim is reported, the relevant material may need to be kept before the routine deletion cycle removes it. **Preserve for claim** means placing a narrow, relevant copy under controlled retention—not suspending deletion for an entire system by default.

Once there is a preservation need:

1. Identify the relevant cameras, date and time range as precisely as possible.
2. Export the minimum segment needed, using an approved method that retains useful metadata where available.
3. Store it in a restricted, secure location separate from general shared drives or personal devices.
4. Record who created the export, when, from which system, and whether it is a working copy or an original.
5. Restrict access to people with a defined role in the incident, claim or authorised review.
6. Set a review or deletion date, and document any reason to keep the material longer.

Preservation is not permission to circulate footage. Do not email raw clips around, send them through personal messaging accounts or place them in a shared folder without access controls and a deletion date. Ask, every time: **Where do exported clips end up, and who can open them?** If you cannot answer confidently, pause the export and fix the storage and access arrangements first.

Review, redact and disclose proportionately

Before any viewing or disclosure, review the footage for people and information unrelated to the incident. A copy may be appropriate in some cases, but so may a controlled viewing, a redacted extract or another response. Consider the requester's rights, the rights and safety of others, and any legal or regulatory duties that apply. Do not promise a particular outcome before the request has been assessed.



Where practical and appropriate, **blur bystanders** before providing a copy. Check more than faces and vehicle registration plates. A person can sometimes be identified through clothing, a name badge, a distinctive mobility aid or their role in a small building community. Also look for screens, paperwork, access codes, keys, unit numbers, reflections and sensitive activities visible in the background.

Quick redaction checklist

- Faces, plates and other clear identifiers of uninvolved people.
- Name badges, uniforms or distinctive items that identify someone in context.
- Children or vulnerable people, with extra care around identification.
- Access-control details, keypads, credentials and security procedures.
- Private documents, computer screens, unit numbers or revealing reflections.
- Audio, if present, including unrelated conversations or sensitive information.
- Any frames at the start or end of an export that reveal unrelated activity.

Redaction must be effective. A black box placed over a face in a still image may not protect the person if the original video, an unredacted frame or identifying audio remains accessible. Use a tool and export process that permanently obscures the selected information in the version being disclosed. Keep any unredacted preservation copy separately, with tighter access.

Ownership and governance: decide who can approve what

In a mixed-use building, cameras may be installed or operated by a property manager, owners' association, landlord, concierge contractor or commercial occupier. Responsibility should not be guessed at during an incident. Establish who is responsible for the relevant system, who makes decisions about its [Browse this site](#) use, and who handles requests and disclosures. In some arrangements, several parties have responsibilities; obtain advice on the actual roles rather than relying on labels alone.

A written CCTV policy should set out the purpose of each system, the areas covered, approved users, access logging, retention periods, export controls and the process for requests. It should also identify who can authorise:

- Routine viewing or a search for an incident.
- Preservation beyond the normal deletion period.
- Redaction, release or controlled viewing.
- Disclosure to insurers, solicitors, law enforcement or other third parties.
- Changes to camera placement, field of view or system access.

Do not allow casual viewing out of curiosity. Each access should have a legitimate purpose and be logged, including the person, date, reason, footage accessed and any export made. If a contractor operates the system, make sure their agreement and working procedures cover confidentiality, security, authorised access, incident handling and deletion.

Set retention periods—and make deletion routine

Retention should be defined in advance and tied to the purpose of the surveillance system. There is no universally suitable number of days for every building. Consider how quickly incidents are normally reported, the camera's purpose, available storage, privacy impact and any applicable legal requirements. Publish or otherwise communicate the policy through appropriate privacy information.



Routine deletion should be an actual system process, not a line in a policy that nobody checks. Confirm that automatic overwrite or deletion works, that exported clips do not escape the normal controls, and that backups do not preserve old footage indefinitely. A claim hold should be specific, recorded and periodically reviewed. When the reason to retain a clip ends, securely delete it in line with the applicable policy and obligations, and record the disposal where required.

Stage Good practice Common failure to avoid Request intake Confirm the incident, requester, time and location. Searching or exporting an entire day without a clear need. Preservation Secure a relevant segment and record the hold. Keeping all cameras indefinitely “just in case”. Review Check bystanders, audio and sensitive background details. Assuming faces and plates are the only identifiers. Disclosure Use an approved, proportionate method and log the decision. Emailing raw clips or sharing an unrestricted folder link. Closure Review the hold and delete when retention is no longer justified. Leaving exports in downloads, inboxes or unmanaged backups.

Keep a clear decision record

A concise disclosure log helps the building demonstrate that it handled the request consistently. Record the date received, requester and authority checked, cameras searched, time range, purpose, decision, redactions, approvals, recipient and delivery method. Note if no footage was available or if the recording had already been deleted under the routine schedule. Keep the log itself appropriately access-controlled.

If the request is unclear, unusually broad, disputed or connected with threatened proceedings, escalate it to the privacy lead, insurer or legal adviser. Avoid giving an informal answer that could be mistaken for a final decision. Where a deadline applies, acknowledge the request promptly and explain the next steps without promising disclosure before review.

From incident response to better camera practice

A slip-and-fall request is also a useful prompt to check whether the system is designed and governed well. Can staff identify the right camera and export a limited segment without exposing the rest of the archive? Are camera views still necessary and proportionate? Do users know not to watch footage out of curiosity? Are routine deletion and access logs working as intended?

Good surveillance practice is not about collecting more footage or making every clip available. It is about having a defined purpose, a controlled field of view, disciplined access, a reliable retention schedule and a careful response when a real incident occurs. Limit the footage to what matters, **preserve for claim** when justified, and protect bystanders through effective review and redaction.

Share this guide

For property teams and building boards, share the article using Facebook share or X (Twitter) share.