

Before sharing CCTV footage, ask two questions: **What security question does this camera answer?** And **who genuinely needs to see the clip?** In a residential block, mixed-use building or shared car park, a recording may capture far more than the incident being reviewed. Residents walking home, visitors, delivery workers, number plates, access codes and private conversations can all appear in the same frame.

Blurring is one practical way to reduce unnecessary exposure, but it is not a substitute for deciding whether footage should be shared at all. The safest approach is to limit collection, limit access and disclose only what is necessary for a defined purpose. This guide explains what to blur, how to govern decisions and what to check before releasing a clip.

Start with the purpose, not the editing software

CCTV should serve a specific, documented security or safety purpose. A camera might help establish how a vehicle entered a garage, whether a fire door was obstructed, or what happened in a lift lobby during a reported incident. It should not be installed or viewed “just in case”, or used to satisfy curiosity about residents and visitors.

Before exporting a clip, write down the reason for the disclosure, the intended recipient and the minimum footage needed. If a short section from one camera [realitytimes](#) answers the question, there may be no justification for sharing a longer recording from several cameras.

Data minimisation begins before anyone opens an editing tool. Camera placement and field of view matter: a lens aimed at a building entrance should not unnecessarily capture the inside of a neighbouring home, a changing area or a wide section of public pavement. Privacy masking, camera repositioning and narrower views can reduce the amount of sensitive material collected in the first place.

What should usually be blurred?

Review the footage from beginning to end, including the moments before and after the main event. Blurring should cover people and details that are not needed to explain the incident, while preserving relevant evidence. The right decision depends on the purpose, recipient and context; there is no universal blur-everything rule.

What may appear When to consider blurring Practical check Faces When people are incidental to the event or do not need to be identified by the recipient. Check reflections, screens and repeated frames, not only the clearest view. Vehicle number plates When the plate is not necessary to the purpose of the disclosure, or identifies an unrelated person. Review parked vehicles, moving vehicles and plates visible in reflections. Bystanders When residents, guests, workers or passers-by are not relevant to the incident. Redact bystanders throughout the clip, including in the background. Private details When door-entry codes, keypads, documents, screens or home interiors are visible. Pause on still frames and inspect the edges of the image. Audio When speech is not needed and could reveal private conversations or sensitive information. Consider muting or removing audio rather than sharing it by default.

Blur faces and redact bystanders

If a clip is being shared with a resident, insurer, contractor or wider audience, consider whether people who are not part of the incident can be identified. To **blur faces**, the edit needs to follow each person’s movement for the entire time they are visible. A blur that slips off a face for even a few frames may defeat the purpose.

“Bystander” can include more than someone standing in the background. It may include a neighbour entering a lift, a cleaner crossing a corridor, a delivery worker at the entrance or a child passing through a garage. **Redact bystanders** where their identity is not necessary to the disclosure. Check that clothing, name badges or other distinctive details do not undermine the redaction if identification remains a concern.

Blur license plates when they are not needed

To **blur license plates**, track vehicles through the full clip, including when they enter or leave the frame. A plate may be reflected in glass or visible in another camera angle. If the plate is relevant to an investigation, restrict the unredacted original to authorised people and consider sharing a redacted copy with anyone who does not need the identifying detail.

Do not overlook incidental information

Faces and plates are easy to spot, but they are not the only details that can expose people or weaken building security. Use a small redaction checklist:

- Door-entry codes, fob readers, keys and security procedures.
- Letters, parcels, screens, visitor logs or paperwork with names or contact details.
- Views into homes, offices or other spaces where people reasonably expect privacy.
- Children, vulnerable people or people receiving assistance.
- Audio that captures a private conversation, access code or other sensitive information.
- Dates, times or location details that could reveal a person’s routine when combined with other information.

Choose the right audience and the right version

Sharing footage with the police to report an incident is different from showing it to a residents’ group or posting it online. The recipient’s role and the purpose of the disclosure should determine what is shared. A person authorised to investigate may need details that a general audience does not. When in doubt, pause and consult your organisation’s privacy lead or legal adviser rather than circulating the raw clip.

Do not assume that a recipient can freely forward footage because they are a board member, employee or resident. Set clear limits: who may view it, whether it may be copied, how long they may keep it, and how they should return or delete it. Raw clips should not be emailed around or dropped into a shared folder without access controls and a deletion date.

Ownership and governance: who decides?

In a managed building, CCTV decisions should have an accountable owner. Depending on the arrangement, that may be the property owner, management company, homeowners’ association or another designated organisation. The board may set policy, but that does not mean every board member should have routine access to footage. Onsite staff and security contractors should follow written instructions rather than making informal disclosure decisions.

Document who is responsible for:

- Approving the camera purpose, position and field of view.
- Authorising access to live feeds and recorded footage.
- Reviewing requests and deciding whether disclosure is appropriate.

- Producing and quality-checking redacted copies.
- Recording disclosures, managing complaints and arranging deletion.

Keep a disclosure log. Record the request, reason, date, footage covered, recipient, decision-maker, redactions applied, transfer method and agreed deletion date. A log helps the organisation show that decisions were consistent and purpose-led, rather than driven by convenience or personal interest.

Secure the exported clip

Before exporting, ask: **Where will this clip end up, and who can open it?** Choose a controlled transfer method with access limited to the named recipient. Avoid personal messaging accounts, open links and folders that inherit broad permissions. If a password or access code is needed, send it separately through an appropriate channel.



Keep the original recording securely and create a separate redacted copy for sharing. Give the copy a clear filename that identifies its purpose without unnecessarily naming people. Check the export on the device or platform the recipient will use: some formats, previews or thumbnails can expose content that looked hidden during editing.



Check that redactions are permanent

A black box placed over a face in a document or image may sometimes be moved or removed if the file has not been flattened properly. Use a redaction process that permanently removes or obscures the underlying information in the shared copy. Review the final exported file—not just the editing screen—and confirm that the original remains protected separately.

For video, watch the full edited clip at normal speed and inspect key frames. Check that blur follows moving subjects, covers reflections and does not disappear during transitions. If the edit is unreliable, shorten the clip, crop the frame where appropriate, or use a still image with more dependable redaction.

Retention and routine deletion

Set a retention period that matches the documented purpose and applicable requirements. Keep routine recordings only as long as needed, then delete them on a regular schedule. When an incident is reported, preserve only the relevant footage for the time needed to handle that matter; do not treat every recording as permanent evidence.

Apply the same discipline to exported clips. A shared copy can outlive the original if it is left in an inbox, phone gallery or cloud folder. Record when it should be deleted, who is responsible and how deletion will be confirmed. Review access permissions and remove them when the purpose ends. A shared folder without an owner or deletion date is not a retention policy.

Before sharing: a practical checklist

1. **Confirm the purpose:** What specific safety or security question does the clip answer?
2. **Minimise the footage:** Select the shortest relevant period and the necessary camera views.
3. **Choose the recipient:** Confirm their role and why they need access.
4. **Review the whole clip:** Look for faces, plates, bystanders, audio, reflections and sensitive details.
5. **Redact and verify:** Check the exported copy frame by frame where needed.
6. **Secure the transfer:** Limit access and avoid informal circulation of raw footage.

7. **Log and delete:** Record the disclosure and set a date to remove the shared copy.

Do not publish an incident clip to social media

Social platforms are designed for broad sharing, not controlled evidence disclosure. Posting CCTV on a public page can expose people who had no connection to the incident and make it difficult to control copies. A redacted clip may still reveal someone through their clothing, location, timing or the people around them. If a request is about an incident, use an authorised, limited disclosure route instead of posting footage publicly.

For sharing this article—not CCTV footage—you can use Facebook share or X (Twitter) share. Add the article URL to the Facebook share link when publishing.

Common publishing mistake: no prices listed

Some scraped articles appear with a note such as “No prices listed”. That is not a CCTV redaction rule or a disclosure requirement; it is usually a content or product-data issue in the source page. Do not add invented prices to fill the gap. If a page genuinely needs pricing information, verify it with the provider and label it clearly. Otherwise, remove the irrelevant note so readers can focus on the privacy and security guidance.

Make sharing the exception, not the habit

The best redaction is often the exposure you never created. Aim cameras carefully, narrow their field of view, restrict access and delete routine footage on schedule. When an incident does require a disclosure, share only what the recipient needs, blur faces and license plates where appropriate, redact bystanders, and keep a record of the decision.

That process protects residents and visitors while preserving footage for legitimate security work. If the purpose, recipient or redaction is unclear, stop before sending—and ask again: **What security question does this camera answer?**