Building security cameras can help investigate incidents, protect people and property, and support a safer environment. But more recording does not automatically mean more security. A camera that captures every doorway, pavement and neighbouring window may collect a great deal of personal information without answering a clear security need.

Data minimisation means collecting and keeping only the personal information needed for a defined purpose. For building surveillance, it is a practical way to decide whether a camera is needed, what it should see, who may access its footage and when that footage should be deleted. The guiding question is simple: *What security question does this camera answer?*

This guide explains how to apply data minimisation surveillance principles in residential and mixed-use buildings, from camera placement to routine deletion. It is general operational guidance, not legal advice; building owners and managers should check applicable privacy law and obtain advice where needed.

What Does Data Minimisation Mean in Building Surveillance?

In practice, data minimisation means designing a camera system around a specific, legitimate security purpose rather than recording broadly "just in case". If the concern is unauthorised entry through a particular door, the camera should normally be configured to capture that entrance—not every person using the lobby, the street outside or the interior of nearby homes.

Applying data minimisation surveillance principles involves more than choosing a camera with a narrow lens. It includes the full information lifecycle:

- **Purpose:** Define the security issue the camera is intended to address.
- **Scope:** Limit the area and detail recorded to what is necessary for that purpose.
- **Access:** Restrict viewing and exporting to authorised people with a work-related need.
- **Retention:** Keep footage only for a justified period, then delete it routinely.
- **Governance:** Record who approved the system and who is responsible for reviewing it.

It is a useful distinction: a camera may be capable of recording a wide area, but that does https://realtytimes.com/new-headlines/cctv-in-elevators-and-common-areas-property-manager-responsibilities not mean the building should use its full field of view or retain every recording indefinitely.

Start With a Defined Security Purpose

Before installing a camera—or continuing to operate an existing one—write down the specific problem it is meant to address. "Improve security" is too broad to guide a responsible decision. A more useful purpose might be to investigate repeated damage to a garage access gate or to establish who entered a restricted plant room after an alarm.

Then ask whether a camera is necessary and proportionate. Could improved lighting, a repaired lock, better access control, a concierge procedure or a change to the delivery process address the problem with less collection of personal information? Cameras should not be the default response to every complaint or worry.

Questions to ask before approving a camera

- What incident or credible risk are we trying to address?

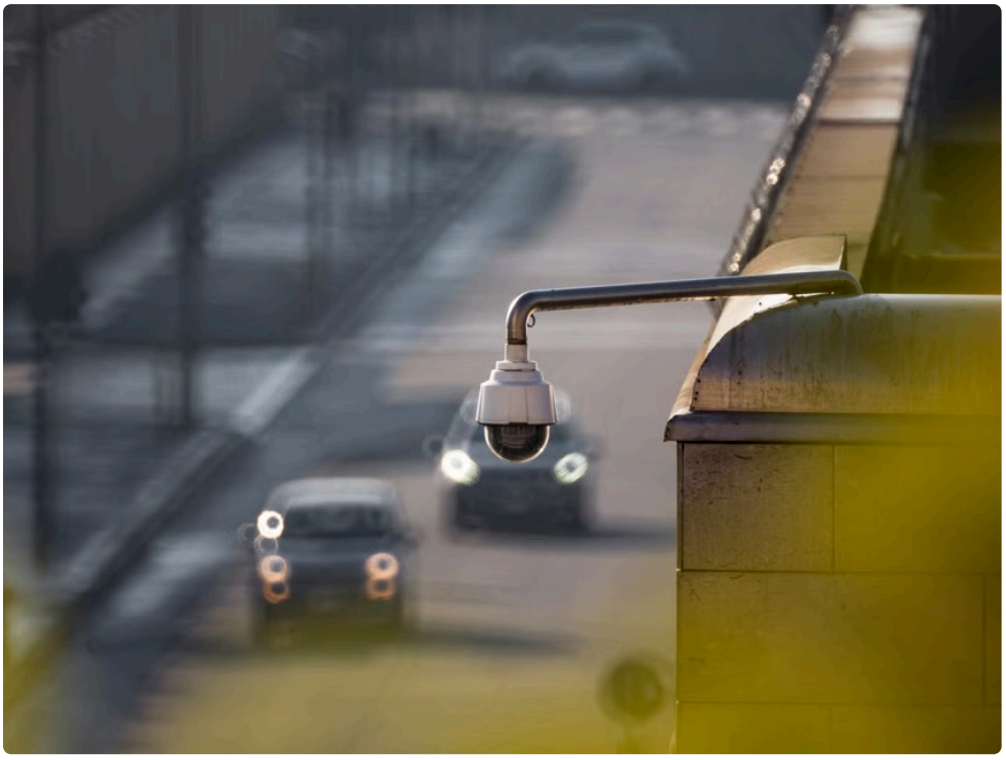
- Where and when is the issue occurring?
- What evidence would the camera need to capture to help investigate it?
- Could a less intrusive measure achieve the same result?
- Who will review whether the camera remains necessary?

These questions help prevent "just in case" cameras—devices installed without a defined purpose and left operating because nobody is sure who can authorise their removal.

Ownership and Governance: Who Decides?

In a managed building, CCTV decisions can involve a freeholder, residents' association or management company, on-site team, security contractor and system installer. A contractor may configure equipment, but responsibility for the decision to collect and use footage should be clearly assigned. It should not be assumed that an installer, concierge or individual resident can decide the purpose and scope alone.

Set out governance in a written CCTV policy or operating procedure. It should identify the responsible decision-maker, describe the approved purposes and camera locations, explain how access is controlled, and state how long recordings are retained. It should also explain how residents, staff and visitors can raise questions or concerns.



For each camera, keep a simple record of its purpose, location, field of view, responsible owner and review date. Record material changes too: for example, if landscaping, a new entrance or a changed building layout means the camera now captures more than it did when installed.

Governance item What to record Purpose The specific security issue the camera addresses Approval Who authorised installation, changes and continued operation Access Which roles may view, export or disclose footage Retention The standard deletion period and any documented exception Review When the camera's need and configuration will next be checked

Camera Placement: Limit the Field of View

To limit CCTV recording scope, position cameras so that they capture the relevant area and as little else as practicable. A camera covering a garage ramp may need to show vehicles approaching a barrier, but it may not need to record neighbouring parking spaces in detail. A lobby camera may be intended to cover an entrance, not to monitor residents sitting in a lounge or reading private correspondence.

Walk the location and check the actual image from the camera—not just the position marked on a plan. Review the view at different times of day, in different lighting conditions and after any changes to the space. Cameras can capture more than expected because of wide-angle lenses, reflections, infrared illumination, movement or a later adjustment to the mounting angle.

Practical ways to reduce unnecessary capture

- Angle the camera towards the relevant doorway, gate or access point.
- Use privacy masking to block areas that do not need to be recorded, such as a neighbour's window or a public-facing section beyond the site boundary.
- Choose a narrower field of view or suitable resolution rather than recording extensive detail without a clear need.
- Disable audio recording unless it is specifically justified and appropriately reviewed.
- Limit recording to relevant zones or times where the system and security purpose support that approach.
- Recheck the view after maintenance, repositioning or software changes.

Privacy masks and camera settings should be tested. A mask that appears in a live view may not necessarily be applied to exported footage in the same way, depending on the equipment. Confirm how the system works before relying on a setting as a safeguard.

Collect Only What Is Necessary—and Keep It Secure

The principle to **collect only what is necessary** applies to access as well as recording. Most staff do not need to browse camera feeds. Casual viewing—because someone is curious, a resident is recognisable or a colleague asks what happened—is not a sound access reason.

Give permissions according to job responsibilities. Separate the ability to view footage from the ability to export or disclose it where the system allows. Use individual accounts rather than shared logins, and keep a record of searches, playback and exports. Regularly review access when staff roles change or contractors leave.

Also decide where exported clips end up and who can open them. Avoid raw clips being emailed around or placed in a shared folder without restrictions. Use an approved, access-controlled method of transfer, share only the relevant excerpt, and record the recipient, reason and date. Set an expiry or deletion date for copies, including working copies created during an incident review.

When preparing a clip for disclosure, consider whether other information can be removed or obscured. A redaction checklist should go beyond faces and number plates. Depending on the scene, check for apartment numbers, access codes, screens, paperwork, keys or fobs, children, staff name badges and audio that reveals a private conversation. Keep an unaltered original securely if needed for a legitimate investigation, and document the relationship between the original and redacted copy.

Set Retention Periods and Delete Footage Routinely

Retaining footage “until the storage fills up” is not a retention policy. Nor is keeping recordings indefinitely because they might become useful one day. Set a standard retention period based on the purpose, the practical time needed to discover and report incidents, and applicable legal requirements. A building should be able to explain why its chosen period is appropriate.

Configure the system to overwrite or delete footage automatically at the end of that period. Check that deletion actually happens, including on any server, backup or secondary device where recordings may be stored. If a specific clip must be kept for an active incident, complaint or legal process, isolate that clip, document why it is being retained, restrict access and set a review point. The exception should not turn into a reason to keep the entire camera archive.

A simple retention and deletion routine

1. Set and approve a standard retention period for each system or category of camera.
2. Enable automatic overwrite or deletion and test the configuration.
3. Keep an incident log for clips preserved beyond the standard period.
4. Review preserved clips regularly and delete them when the reason to retain them ends.
5. Record routine checks and any deletion failures or corrective action.

Routine deletion is an essential part of data minimisation surveillance. It reduces the amount of information that could be exposed in a breach, misused by an unauthorised viewer or requested for a purpose unrelated to building security.

What About Costs? Why This Article Does Not List Prices

A common mistake in scraped articles is to include a price heading and then provide no prices—or to repeat a figure without explaining what it covers. CCTV costs vary according to the number and type of cameras, cabling, storage, network requirements, access-control integration, installation conditions, maintenance and support. A single figure without those details can be misleading.

This guide does not list prices because it is about the data-minimisation decisions that should come before a purchase. When comparing quotations, ask suppliers to specify equipment, installation, storage capacity, retention configuration, user permissions, export controls, maintenance and any ongoing fees separately. Include privacy masking and secure handling of exported clips in the requirements, rather than treating them as optional extras after installation.

Review the System, Not Just the Hardware

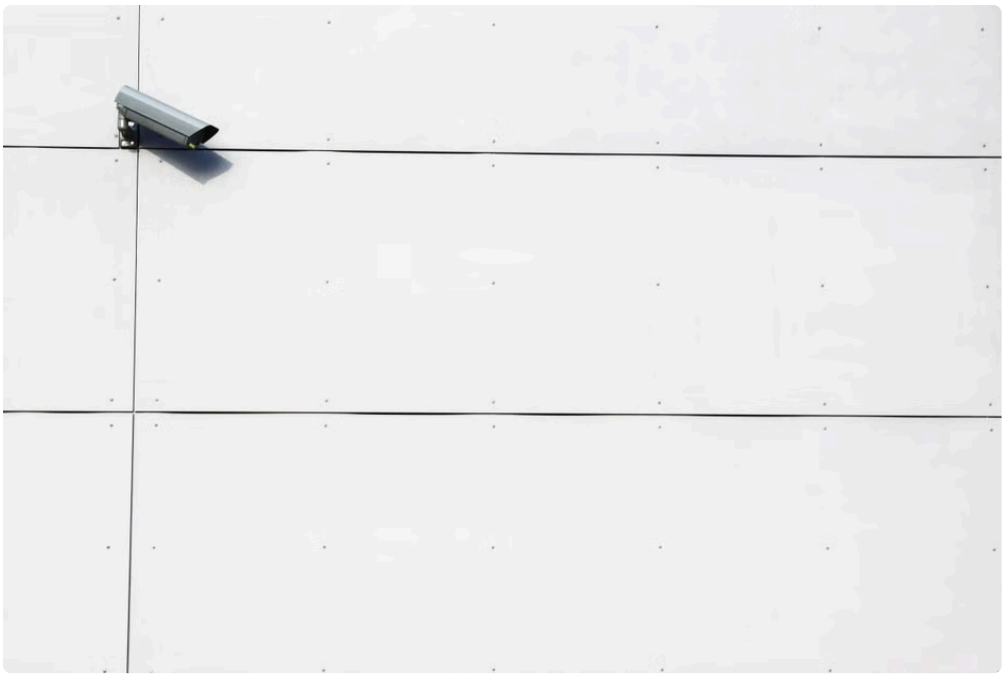
A camera that was justified several years ago may no longer be necessary. The original problem may have stopped, access arrangements may have changed, or the device may now capture an area that was not part of its original field of view. Schedule a review with the appropriate building decision-makers and involve on-site staff who understand how the space is used.

For each camera, revisit the purpose, necessity, placement, access list, retention settings and complaints or incident history. If the camera no longer answers a meaningful security question, consider narrowing its view, changing its settings or removing it. Good governance includes being willing to do less recording.

Conclusion: Make Every Camera Earn Its Place

Data minimisation for building cameras is a practical discipline: define the security purpose, limit CCTV recording scope, collect only what is necessary, control access, and delete footage on a routine schedule. It also means deciding who owns and governs the system, documenting exceptions and checking where every exported clip goes and who can open it.

The best starting point is not “Where could we install another camera?” It is: **What security question does this camera answer, and can we answer it with less recording?**

Share This Guide

Share on Facebook | Share on X (Twitter)