

Residents are more likely to trust a CCTV system when they can understand what it does, what it does not do, and who is accountable for it. They are less likely to trust vague promises such as “your safety is our priority” if nobody can explain where cameras point, how long recordings are kept, or who can watch them.



The aim is not to persuade residents that surveillance has no privacy impact. It does. The aim is to explain the impact honestly, show that recording is limited to a defined purpose, and make the rules easy to find. A clear **plain language notice** is a good start, but it should reflect real operating practices—not simply sound reassuring.

Before writing or updating a notice, ask one practical question: **What security question does this camera answer?** If there is no clear answer, pause and review whether the camera is needed, where it is aimed, and whether a less intrusive option would work.

Start with the reason, not the reassurance

Residents want to know why cameras are operating in their building. State the specific purpose in ordinary language, such as investigating reported incidents, helping manage access to a shared entrance, or understanding a safety incident in a garage. Avoid broad claims such as “for security purposes” on their own: they do not tell residents what the system is actually for.

This is the idea behind **purpose limited recording**. A camera installed to investigate damage in a car park should not quietly become a way to monitor whether residents are using a space in a preferred manner. If a proposed new use comes up, it should be assessed and communicated rather than assumed to be covered by the original notice.

Be precise about limits, too. If the system is not monitored live, say so. If cameras do not record audio, say that. If footage is not used to track residents’ day-to-day movements, explain that as an operational rule only if it is true and can be enforced.

Explain who makes the decisions

“The CCTV company looks after it” is not a complete answer. A contractor may install equipment, host footage or provide technical support, but residents should be able to identify the organisation responsible for deciding why and how the system is used. Depending on the building’s arrangements, that may be the owners’ association, property manager, landlord or another organisation. Confirm the appropriate role for your building rather than guessing.

Explain the governance in a simple, practical way:

- **Who approved the system?** Name the responsible organisation or decision-making body, and describe how significant changes are considered.
- **Who operates it?** Identify the onsite role or service provider responsible for routine administration.
- **Who can access footage?** Describe the roles authorised to review recordings and the circumstances in which they may do so.
- **Who handles questions?** Provide a monitored contact route for privacy queries, access requests and complaints.

It can help to explain that access is not granted just because someone is curious, is a resident, or sits on a committee. There should be a defined reason, a permitted role and a record of access. Committee members should not be given informal access to a live feed or recordings simply because the cameras are in a shared building.

Show where cameras point—and where they do not

Camera placement is one of the most visible signs that privacy has been considered. A notice that says “cameras are carefully positioned” is less convincing than a clear explanation of the areas covered, the areas excluded and the controls used to limit the view.

Describe locations in terms residents recognise: the main entrance, a lift lobby, a parcel area or a vehicle entrance. Avoid publishing detailed security layouts if doing so could create a separate safety risk. You can still explain the general coverage and provide a suitable route for residents to ask for more information.

Field of view matters as much as camera location. A camera can capture spaces beyond the property boundary or areas where people reasonably expect greater privacy. Review each view on site, not just on a plan. Consider whether the lens can be repositioned, zoom restricted, or privacy masking applied to exclude windows, neighbouring property or unrelated areas. Masks should be checked after any equipment adjustment.

Audio recording is particularly intrusive. Do not enable it by default or leave it on because the equipment supports it. If audio is proposed, assess whether it is necessary and proportionate, check the applicable requirements, and explain it plainly. If audio is not used, state that clearly in the notice.

A quick placement check

- Does each camera address a specific, documented security or safety concern?
- Can it be aimed at the concern without capturing more of the area than necessary?
- Are neighbouring homes, windows and private spaces excluded or masked?
- Could lighting, access control, a mirror or an onsite procedure address the issue with less recording?
- Who will recheck the view after repairs, replacement or repositioning?

Make retention and access easy to understand

A **retention and access summary** should answer two direct questions: how long is footage normally kept, and who may view it? Do not rely on phrases such as “kept as necessary” without giving residents a normal retention period or explaining the limited exception for an incident that needs to be preserved.

Choose a retention period based on the building’s actual needs, the time usually taken to report an incident and the applicable requirements. There is no single number that suits every building. Avoid retaining all footage indefinitely “just in case”. Routine deletion should happen automatically where possible, and the process should be checked to confirm that it is working.

If a relevant incident is reported, a specific clip may need to be preserved while it is reviewed or handled. Explain that this is an exception, not a reason to keep the entire recording system’s footage for longer. Record why the clip was retained, who authorised it, where it is stored and when its continued retention will be reviewed.



Resident question What a useful answer should say How long is routine footage kept? Give the normal period and explain that recordings are then routinely overwritten or deleted. Who can watch it? Identify authorised roles and say that access is limited to defined purposes. Can footage be shared? Explain that disclosures are considered individually and handled through an approved process. What happens after an incident? Explain how relevant footage may be secured, reviewed and given a review or deletion date.

Know where exported clips go

Live camera access is only part of the privacy picture. A clip exported for an incident can create another copy that is easier to share, lose or keep too long. Always ask: **Where do exported clips end up, and who can open them?**

Set a controlled process for exports. For example, require an authorised person to document the reason, the footage selected, the recipient, the storage location and the planned deletion date. Use approved, access-controlled storage. Avoid emailing raw clips around or putting them in a broadly shared folder with no owner and no deletion date. If a clip must be provided to an external party, confirm the basis and the recipient through the appropriate process, and keep a record.

Limit access to the smallest group that can do the job. Use individual accounts rather than shared logins where available, review permissions when staff or contractors change, and keep access logs. Residents do not need a

technical manual, but they should be able to see that the building has practical controls rather than relying on goodwill.

Explain data minimisation in everyday terms

Data minimisation means collecting only what is needed, in the places and for the period needed. Put it into everyday language: “We use cameras in selected shared areas to help review reported incidents. We do not record every part of the building, and routine footage is deleted after the stated period.” Only use wording that accurately describes the system.

Also consider information beyond faces and vehicle registration plates when footage is shared or disclosed. A small redaction checklist should cover:

- faces and plates of people or vehicles not relevant to the matter;
- apartment numbers, access codes, fobs or other visible security details;
- screens, paperwork or parcel labels that reveal personal information;
- private windows, neighbouring properties and unrelated areas in the frame; and
- audio or background conversations, if audio is lawfully recorded.

Redaction is not just a technical task. Someone should check the finished copy before it is sent, confirm that the obscured details cannot be recovered from the file, and retain the original only under the building’s controlled process.

Use a notice residents can actually act on

A sign beside a camera should be short enough to read and should identify who is responsible and where to find fuller information. It is not a substitute for a more complete privacy notice. Make that notice available in a place residents already use, such as the resident portal, building reception or management office. Offer a contact route that is monitored and explain what residents should include when reporting an incident or asking a question.

Here is a starting point to adapt to your building:

CCTV in this area: The building’s [responsible organisation] operates cameras in selected shared areas to help review reported safety and security incidents. Cameras cover [general locations]. They are not used to monitor residents’ everyday activities. Audio is [not recorded / recorded only as explained in the full notice]. Routine footage is kept for [period] and then automatically overwritten or deleted. Access is limited to authorised people for defined purposes. For details, questions or a privacy request, contact [role and contact details] or read the full CCTV privacy notice at [location].

Check every statement against the actual settings and procedures. If the building does use live monitoring, or there is an exception to the usual retention period, explain it rather than using a template that suggests otherwise.

Be transparent about costs without inventing them

Some scraped or republished articles are flagged because no prices are listed. For a resident privacy explainer, invented CCTV prices would be misleading and are not a substitute for explaining the privacy controls. This article does not list prices because costs depend on the building and the equipment or service being discussed.

If residents are being asked to approve a new system or a paid change, separate the privacy explanation from the financial proposal—but link them clearly. The proposal should state relevant installation, maintenance or service

costs where known, who pays, and how the decision will be made. Do not imply that a privacy measure is free if it is not, and do not use an absent price as a reason to avoid explaining the system's purpose or governance.

Make the explanation a living commitment

Trust is built when the notice matches what residents can observe and when staff follow the rules consistently. Review the camera purpose, field of view, access list, routine deletion and exported-clip process on a schedule and after a material change. Record the review and assign someone to fix any gaps.

Finally, invite questions without treating them as opposition. A resident asking why a camera sees a particular area may have noticed a genuine problem. A straightforward answer, a documented decision and a willingness to adjust an unnecessary view will do more for confidence than reassuring language alone.

Share this article

Share on Facebook | Share on X (Twitter)

Replace the example.com links with the published article URL before sharing. This guidance is general information, not legal advice; check current UK data protection requirements and obtain appropriate advice for your building's circumstances.