

Yes—usually. A tenant’s camera system should not be treated as though it were simply another part of the building’s CCTV network. The tenant and building owner may have different purposes, responsibilities, access rights and retention needs. If those differences are not made clear, a system installed to protect one office can end up capturing shared corridors, monitoring other occupants or creating uncertainty about who controls recorded footage.

The practical starting point is a simple question: **What security question does this camera answer?** If there is no specific, proportionate answer, the camera may not be needed. When a tenant does have a sound reason for installing cameras, written rules should explain what they may capture, who makes decisions about the system, who can view or export recordings, and when the footage must be deleted.

This is not just a matter of keeping the landlord’s CCTV policy tidy. It is about managing **tenant camera systems** with clear boundaries, and agreeing a **lease allocation of control** that works in practice.

Why tenant cameras need their own rules

Building CCTV is often installed and managed for shared purposes: for example, monitoring an entrance, lift lobby, loading area or car park. A tenant’s cameras may serve a narrower purpose, such as protecting stock in a private reception area or controlling access to a restricted room. The fact that both systems use cameras does not mean they should share the same rules.

Different systems may have different operators, storage locations and users. A building manager might use a security contractor, while a tenant’s facilities team manages its own cameras. Without separate arrangements, it can be unclear who is responsible for responding to a request for footage, handling a complaint or checking that recordings are deleted on time.

In the UK, organisations using identifiable CCTV footage will generally need to consider data protection requirements, including the UK GDPR and Data Protection Act 2018. The precise responsibilities depend on the circumstances, so seek advice where roles or [realtytimes.com](https://www.realtytimes.com) purposes are unclear. A landlord and tenant should not assume that one party automatically takes responsibility just because the cameras are physically inside the building.

Agree who controls decisions and footage

Start by mapping who decides why each camera is used and how it operates. For each system, record who determines its purpose, placement, field of view, access permissions and retention period. That decision-making role is central to a clear **lease allocation of control**.

A lease or separate camera agreement can set out what the tenant is allowed to install and what approvals it needs. It can also clarify that permission to install equipment does not automatically give the tenant access to the building owner’s recordings—or give the owner routine access to the tenant’s footage.

Decision or task Questions to settle Purpose What specific security need does the system address, and who approved it? Installation Who approves the equipment, location, cabling and any changes? Access Which named roles can view live feeds or recorded clips? Exports Who can export footage, where does it go, and who can open it? Retention How long is footage kept, and how is routine deletion checked?

Where the landlord and tenant genuinely determine the purposes and means of a system together, their responsibilities may require a more formal arrangement. Do not use a generic clause to paper over shared

decision-making. Get suitable legal or data-protection advice and document the actual working arrangements.

Keep camera placement and field of view tight

One of the most common problems is a camera installed for a private purpose that also captures a shared corridor, neighbouring office entrance, reception desk, lift lobby or public-facing area. A tenant may only intend to monitor its own doorway, but a wide-angle lens can record people passing through the building throughout the day.

Set placement and field-of-view limits before installation, not after a complaint. Ask the installer to show the proposed view and, where practical, test it during normal building operations. Use privacy masking or camera angles to exclude areas that do not need to be recorded. Recheck the view if furniture, partitions or the camera itself moves.

A useful approval process should ask:

- Which exact area needs monitoring, and why?
- Can the same purpose be met with a narrower view, access control or improved lighting?
- Will the camera capture shared or neighbouring areas? If so, can those areas be masked?
- Is audio recording enabled? If it is not necessary, disable it.
- Will the view change at different times, or when the camera pans or zooms?

Data minimisation is more than choosing a small number of cameras. It means limiting what is collected to what is needed for a stated purpose. Avoid cameras installed “just in case”, and do not use a camera’s full capabilities simply because they are available.

Set separate access policies

Different systems call for **separate access policies**. A person who can view the building’s lobby cameras should not automatically be able to view a tenant’s private system. Equally, a tenant’s security staff should not be given access to shared building cameras unless there is a clear, documented reason.



Keep access limited to people who need it for their duties. Use individual accounts rather than shared logins, review permissions when staff change roles or leave, and keep an access log where the system supports it. Viewing footage out of curiosity is not an acceptable reason to open a camera feed.

Control exports as carefully as viewing

Viewing a clip is not the same as exporting it. Exported footage can be copied, forwarded or stored beyond the camera system's controls. Before authorising an export, record why it is needed, which footage is being released, who approved it and who will receive it.

Always ask: **Where do exported clips end up, and who can open them?** Prefer a controlled, access-restricted destination with an expiry or deletion date. Avoid raw clips being emailed around or placed in a shared folder with no named owner and no deletion date. If footage is being shared with police, insurers, lawyers or another party, use an approved secure method and retain a note of the disclosure.

Choose a retention period and delete routinely

There is no single retention period that fits every camera system. Set a period that is justified by the purpose and operational need, then configure the system to overwrite or delete footage automatically where possible. Longer storage should not become the default just because a device has plenty of capacity.

Document the routine period and the process for any exception. If footage must be preserved for a specific incident, isolate only the relevant material, record who authorised the hold and why, and review it when the matter is resolved. Do not keep an entire system's recordings indefinitely because one clip is under review.

Routine deletion needs an owner. Decide who checks that the settings work, how often they are reviewed and what happens when equipment is replaced or a tenant leaves. A useful policy should cover recordings held on local devices, cloud services, exported files and backups where relevant—not just the main recorder.

Put the rules in the lease or a camera agreement

The lease may be the right place to set the broad requirements, while a schedule or separate agreement can hold technical details that may change. The documents should work together and identify who must approve installation and changes. Avoid vague wording such as "cameras are permitted subject to management approval" if it leaves basic questions unanswered.

Consider covering:

- Permitted purposes and prohibited uses, such as monitoring staff performance without a properly assessed basis.
- Approval requirements for camera positions, field of view, audio, analytics and changes to equipment.
- Who operates the system and who can access live or recorded footage.
- Export, disclosure, security and record-keeping procedures.
- Retention periods, routine deletion and incident-related holds.
- Signage and how people can find information about the system.
- What happens when the lease ends, including removal of equipment and deletion or transfer of recordings.

Make sure the written rules match what happens on site. A policy that says only two people have access is not useful if several teams share one login. Likewise, a stated deletion period is not effective if exported clips remain on an unmanaged drive.



Review the system when circumstances change

A camera that was appropriate when a tenant moved in may become excessive after a layout change or a new security arrangement. Review systems periodically and whenever the purpose, equipment, field of view, users or building layout changes. Keep a simple camera register recording the system owner, purpose, location, viewing area, retention period and access roles.

For a complaint or incident, preserve only what is relevant and follow the agreed disclosure process. Do not hand over footage informally because someone asks for it. Check the request, authority and scope, and consider whether other people in the clip need protection through cropping, masking or another appropriate redaction. Redaction checks should go beyond faces and number plates: screens, access codes, documents, name badges and sensitive conversations may also be exposed.

What about installation costs and prices?

There is no reliable, universal price for a tenant camera system. Costs depend on the number and type of cameras, cabling, storage, installation conditions, software, access controls and ongoing support. This article does not list prices, and a figure without a site assessment could be misleading. Ask for an itemised quotation that separates equipment, installation, storage, maintenance and any recurring charges. Include the cost of secure access, routine deletion and administration—not just the cameras.

A practical checklist before approving tenant cameras

1. Write down the specific security purpose and consider less intrusive alternatives.
2. Confirm who controls the system and document the lease allocation of control.
3. Approve a precise location and field of view; mask areas that are not needed.
4. Set separate access policies for tenant and building systems.
5. Limit, log and secure exports; name the recipient and set a deletion date.

6. Choose a justified retention period and test that routine deletion works.

7. Review the arrangement when equipment, occupants or building layouts change.

Tenant-operated cameras can be appropriate, but they need clear boundaries. The aim is not to prevent reasonable security measures; it is to ensure each camera has a defined purpose, captures no more than necessary and is governed by people who understand their responsibilities. If the purpose, access or deletion process is hard to explain, pause and resolve those points before installation.

Share this article

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