



Guidance for Community Residents – Your rights to Privacy

Individuals have specific rights regarding their personal data capture by CCTV systems, including the right to access footage and to request its deletion under the General Data Protection Regulations 2018 (GDPR)

Your rights to Privacy

Are you concerned with the way some organisations use CCTV to record data during activities including sports and fitness classes (e.g. badminton, yoga, dance) and activities involving mothers with young children or life drawing classes?

Are you aware of your rights for reasonable privacy?

Background

Many organisations install CCTV systems for crime prevention and security purposes. These systems are now widely used, and people generally acknowledge their presence within communities.

However, not all organisations implement CCTV systems with the primary objective of protecting the privacy of individuals using their facilities. In certain instances, cameras may be placed in locations where users could reasonably expect a degree of privacy.

This guide was created at the request of residents who reported privacy concerns to the parish council.

This guide has been prepared to provide clear information about your rights when an organisation collects your data through CCTV, especially in instances where you believe the monitoring may be unreasonable or infringe upon your privacy.

What does an acceptable CCTV plan look like?

A typical CCTV plan includes external coverage of the main entrance, car park, and rear access points, with strategically placed internal cameras covering key areas like the kitchen, bar, and main hall entrances, while respecting privacy regulations.

The goal is to deter crime and monitor activity, with clear signage informing visitors of the CCTV system's presence, as per the Information Commissioner's Office (ICO) guidelines.

Where you would expect external cameras to be located

- Main Entrance: Essential for monitoring who enters and leaves the hall.
- Car Park: Covers vehicle entry and exit points, and the general parking area to deter vehicle theft or vandalism.
- Side and Rear Entrances: Crucial for securing less visible points of access and protecting against unauthorized entry.
- Sheds and Outbuildings: To secure storage areas and prevent theft or damage to property.

Where you would expect internal cameras to be located

- Kitchen and Bar Areas: High-traffic zones where money handling or valuable equipment may be present.
- Foyer Entrances/Exits: To monitor activity during events.
- Secure Cupboards: Where recording equipment is stored.

Key Considerations

- Privacy: Cameras should be positioned to only capture relevant areas, avoiding private spaces and respecting reasonable expectations of privacy.
- Signage: Visible signs at all entrances and in key locations, such as the kitchen and notice boards, are required by law to inform people about the CCTV system.
- Equipment Security: The recording equipment itself should be stored in a secure, locked location to prevent tampering.

An effective risk assessment might reasonably determine that CCTV cameras are appropriate for installation in foyer areas; however, their use would not be suitable in locations where individuals may have heightened expectations of privacy during activities or events, such as fitness classes or exercise classes, or gatherings involving Mothers with young children.

What to do if you think the CCTV is intrusive and impacting on your rights to privacy

1. Report your concerns to the event/activity provider (i.e. Pilates class instructor)
2. You also have the right to challenge the facility organisation to fully understand their GDPR policy, why they are collecting your data, and how they are collecting and using your data.

Organisations must justify CCTV use under GDPR, showing in their Risk Assessment that security and health & safety needs are balanced with individuals' privacy rights.

How to challenge the facility organisation on their CCTV policy

1. This section lists key questions for understanding an organisation's GDPR policy, data collection reasons, and data management practices.

GENERAL QUESTIONS ABOUT YOUR DATA
Data security & Storage
How is my data being stored?
Who has access to my data?
Data Usage and Purpose
Why is my data being stored?
Is my data being used for other purposes?
Is my data being shared with 3 rd parties?
Data Retention & Deletion
How long will my data be kept?
Can I request my data to be deleted?
Transparency & Control
What data do you have about me?
How do I update or correct my data?
Accountability & Oversight
Who is responsible for managing my data?
What if there is a data breach?

2. This section explains how to request your data from the organisation and file a formal complaint with the Information Commissioner's Office (ICO).

SPECIFIC ACTIONS YOU CAN TAKE	
I don't want to be filmed	Object to an organisation using your data The right to object to the use of your data ICO
I want to see the data you are holding on me	Getting copies of your information Make a subject access request ICO