A Guide to CCTV Use in Pubs and Leisure Premises

Published by SMB Training

Appropriate use of Closed-Circuit Television (CCTV) in pubs, bars, and leisure premises can provide immense benefits to your business, your staff, and the wider community. It is an increasingly vital tool for securing criminal convictions, resolving premises disputes, and assisting emergency services.

However, operating a surveillance system comes with strict legal and regulatory responsibilities. Mismanagement can lead to severe financial penalties, licensing reviews, or even criminal prosecution. At SMB Training, we have put together this practical guide to help operators navigate their ongoing responsibilities seamlessly.

1. Legal and Data Protection Requirements

The use of CCTV must comply directly with UK data protection laws, including the UK GDPR and the Data Protection Act. To remain compliant, operators must ensure that their use of surveillance is always **necessary** and **proportionate** to the issues being addressed.

- **Justification and Documentation:** Before installing or upgrading a system, you must consider whether alternative, less intrusive options are available. For example, installing extensive CCTV in a consistently trouble-free, well-staffed community pub may be difficult to justify under data protection laws. Your decision to use CCTV, along with the specific reasons for it, must be formally documented.
- **Privacy Hotspots:** Cameras should generally never be placed in areas where individuals have a heightened expectation of privacy, such as toilets and changing rooms. Surveillance in these areas can only be justified in truly exceptional circumstances—such as documented, repeated anti-social behaviour or drug-related crime—and must be restricted to a strictly limited timeframe.
- **Audio Recording:** Your system should not record conversations between members of the public. Continuous audio recording is highly intrusive and rarely justifiable under data protection legislation. Where possible, choose equipment without audio capabilities or ensure the function is disabled.

2. Registration and Fees

Every business operating a CCTV system that captures images of individuals must register with the Information Commissioner’s Office (ICO).

- **The Data Controller:** You must name a "data controller"—the entity responsible for managing the footage and determining how it is used or disclosed. In the licensed trade, there may be multiple data controllers. For instance, if a pub company (pubco) and a tenant both have access to or shared responsibility for the video feed, both must be registered.

- **Annual Fees:** Operators are required to pay an annual registration fee to the ICO. Failing to register or maintain your payment risks an immediate fine and potential criminal conviction.

3. Licensing Conditions and the Police

As a licensee, you will frequently interact with local licensing authorities and the police regarding surveillance.

- **Imposed Conditions:** The police may make representations to the licensing sub-committee requesting that CCTV installation be made a formal condition of your premises licence. While licensing authorities hold the power to enforce this, it must still be justified. If your premises has no history of crime, disorder, or anti-social behaviour, a blanket requirement for CCTV may not be legally warranted. You hold a right of appeal to the Magistrates' Court if you believe a condition has been unfairly or disproportionately imposed.
- **Accessing Footage:** If a condition is added to your licence requiring you to maintain a working CCTV system and provide footage to the police or licensing authority upon request, **failing to do so is a criminal offence**. It can lead to a closure order, a review of your premises licence, or prosecution.

4. Handling Footage and Individual Rights

The images captured by your system constitute personal data. Therefore, the public and your staff retain specific information rights.

- **Subject Access Requests (SARs):** Anyone captured on your footage has the right to request a copy of their data. You must respond to a SAR within one calendar month. Generally, you cannot charge a fee for this. When processing a request, you must protect the privacy of third parties; this may require you to redact or blur the faces of other customers or staff before releasing the footage.
- **Retention Periods:** Footage should only be retained for as long as is strictly necessary for your business purposes (typically 31 days, unless required for an ongoing investigation). Implement a system that automatically and securely overwrites older data.
- **Security Measures:** Access to the live monitors and recorded footage must be restricted to authorised personnel only. The physical recording equipment should be kept in a secure, locked location to prevent tampering or unauthorised downloading.

5. Transparency and Practical Setup

Before your system goes live, you must take the necessary steps to ensure transparency and proper technical alignment:

- **Clear Signage:** You must display highly visible, legible signs in the immediate vicinity of your cameras (such as entrances, bar areas, and windows). These signs should clearly state that CCTV is in operation, explain *why* it is being used (e.g., crime prevention and public safety), and provide contact details for the data controller.

- **Camera Angles:** Ensure your cameras are positioned precisely to capture only what is necessary for your operational goals. Avoid capturing excessive footage of public pavements, neighbouring commercial properties, or private residential windows.

Summary Checklist for Leisure Operators:

1. Document your legal justification for installing CCTV.
2. Register as a data controller with the ICO and pay the annual fee.
3. Display clear, compliant signage at all key entry points.
4. Securely restrict access to recording equipment and viewing screens.
5. Train your management team on how to download footage and handle Subject Access Requests within the legal one-month timeframe.