CCTV checklist

Step 1 of 4: Installing a system

1.1 Data protection impact assessment

Your business has identified and documented the potential impact on individuals' privacy and taken this into account when installing and operating the CCTV system. You regularly review whether CCTV is still the best security solution.

▼ More information

> If your cameras are likely to overlook any areas which people would regard as private (eg a neighbour's garden), you should consider where to install them and avoid siting cameras in these locations, or restrict their fields of view or movement to minimise intrusion. For internal workplace cameras, consider the greater expectation of privacy in certain areas such as locker rooms or social areas. Consider the differing impacts of camera technologies. For example, a fixed camera might be more appropriate than a Pan-Tilt-Zoom. A system that records sound will be significantly more intrusive and harder to justify than one without that capability. If your business is sited in a mixed or multiple-use location, consider the privacy concerns of the users of any common spaces.

- (●) Not yet implemented or planned
- ( ) Partially implemented or planned
- ( ) Successfully implemented
- ( ) Not applicable

1.2 Registration

Your business has paid the data protection fee to the Information Commissioner's Office (ICO).

▼ More information

Once you have determined the purpose for which you are processing personal data you must pay the ICO a data protection fee unless you are exempt. If your business uses non-domestic CCTV systems you are likely to need to pay a fee. There are three different tiers of fee and you are expected to pay between £40 and £2,900. The fee depends on the size of your business, your turnover and, in some cases, the type of business you are. If you want to know more, the ICO has published more detailed Guidance on our website .

- (●) Not yet implemented or planned
- ( ) Partially implemented or planned
- ( ) Successfully implemented
- ( ) Not applicable

Next ➜

CCTV checklist

Step 2 of 4: Management

2.1 Governance

Your business has a policy and/or procedure covering the use of CCTV and has nominated an individual who is responsible for the operation of the CCTV system.

▼ More information

> A policy will help you to use CCTV consistently. The policy should cover the purposes you are using CCTV for and how you will handle this information, including guidance on disclosures and recording. It is good practice to assign day-to-day responsibility for CCTV to an appropriate individual. They should ensure that your business sets standards, has procedures and that the system complies with legal obligations including individuals' rights of access.

- (●) Not yet implemented or planned
- ( ) Partially implemented or planned
- ( ) Successfully implemented
- ( ) Not applicable

2.2 Requests for personal data

Your business has established a process to recognise and respond to individuals or organisations making requests for copies of the images on your CCTV footage and to seek prompt advice from the Information Commissioner where there is uncertainty.

▼ More information

> Be aware of people's right to request a copy of their image (including staff) and be prepared to deal with these. These rights exist for both staff and customers. Have a

clear policy that will help you deal with requests effectively. Requests can be made verbally or in writing, so your policy should include how to record any requests you receive verbally. You must provide the Information without delay and at the latest within one month of receipt of the request. An individual should not have any greater difficulty in requesting their data when this is an image compared to a document or computer file. Providing information promptly is important, particularly if you have a set retention period which conflicts with the statutory response period. In such circumstances it is good practice to put a hold on the deletion of the information. When dealing with individual's requests for personal data you should carefully consider information about third parties, just as you would be if they were mentioned in a document or computer file that was the subject of a request. Keeping an accurate log of subject access requests you receive and how you have handled them will help you manage requests and deal with any challenges to how you've handled them. You should not provide images to third parties other than law enforcement bodies to assist them in the detection or prevention of a crime. You should have a process in place to enable you to do this as quickly as possible.

- (●) Not yet implemented or planned
- ( ) Partially implemented or planned
- ( ) Successfully implemented
- ( ) Not applicable

2.3 Training

Your business trains its staff in how to operate the CCTV system and cameras (if applicable) and how to recognise requests for CCTV information/images.

▼ More information

Make all relevant staff aware of your CCTV policy and procedures and train them where necessary. For example: * All staff who are authorised to access the cameras should be familiar with the system, and with the processes for reviewing footage and extracting it if required. * All staff should be familiar with procedures for recognising and dealing with requests for personal data. * All staff should be familiar with the likely disciplinary penalties for misuse of the cameras. * Where a staff member's role explicitly includes monitoring of CCTV, eg a security guard, ensure that you meet and record appropriate training standards (such as SIA qualifications).

- (●) Not yet implemented or planned
- ( ) Partially implemented or planned