



Sirius Ltd
Surveillance and CCTV
Policy Guidelines

To be adapted to your business as appropriate

Contents

1. Surveillance and CCTV Policy
2. Examples of CCTV Usage
3. Location of Camera
4. Recording and Retention of Images
5. Access to and Disclosure of Images
6. Individual's Access Rights
7. Covert Recording
8. Staff Training
9. Implementation

1. Surveillance and CCTV Policy

This policy sets out the use and management of the CCTV equipment and images in compliance with the relevant Data Protection legislation consisting of the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK, unless and until the GDPR is no longer directly applicable in the UK and then any successor legislation to the GDPR or the Data Protection Act 1998 (the Data Protection Legislation) and the CCTV Code of Practice.

The Company uses closed circuit television (CCTV). CCTV is used for maintaining the security of property, premises and for preventing and investigating crime, it may also be used to monitor staff when carrying out work duties. For these reasons, and for health and safety purposes, the information processed may include visual images, personal appearance voice recordings and behaviours. This information may be about staff, customers and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where necessary or required, this information is shared with the data subjects themselves, employees and agents, services providers, police forces, security organisations and persons making an enquiry.

2. Examples of CCTV Usage

- To assist in the prevention or detection of crime or malpractice.
- To assist in the identification and prosecution of offenders.
- To monitor the security of customers' craft.
- To monitor the security of the Company's business premises and equipment.
- To ensure that health and safety rules and Company procedures are complied with.
- To assist in the identification of unauthorised actions or unsafe working practices that might result in disciplinary proceedings being instituted against employees and to assist in providing relevant evidence.

3. Location of cameras

Cameras are located at strategic points throughout the Company's business premises. The Company has positioned the cameras so that they only cover communal or public areas on the Company's business premises and they have been sited so that they provide clear images. Cameras do not focus inside individual cubicle toilets, showers, staff kitchens and designated staff break rooms

All cameras (with the exception of any that may be temporarily set up for covert recording) are clearly visible.

Appropriate signs are prominently displayed so that employees, clients, customers and other visitors are aware they are entering an area covered by CCTV.

4. Recording and Retention of Images

Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images.

Images may be recorded either in constant real-time (24 hours a day throughout the year), or only at certain times, as the needs of the business dictate.

As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in any event, are not held for more than one month. Once a hard drive has reached the end of its use, it will be erased prior to disposal.

Images that are stored on, or transferred onto, removable media are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of one month. However, where an investigation is being conducted, images may need to be retained for a longer period.

5. Access to and Disclosure of Images

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded locally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system and to those line managers who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented. CCTV images can be reviewed at Head Office in real time as well as reviewing previously recorded images.

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service.
- Relevant legal representatives.
- Line managers involved with Company disciplinary and performance management processes.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The CEO/Managing Director of the Company (or another senior director acting in their absence) is the only person who is permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

6. Individuals' Access Rights

Under the Data Protection Legislation, individuals have certain rights to protect and control their data and on request to receive a copy of the personal data that the Company holds about them, including CCTV images if they are recognisable from the image.

If you wish to access any CCTV images relating to you, you must make a written request to the Company's Data Privacy Manager. You will not have to pay a fee to access your personal images. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances. Your request must include the date and approximate time when the images were recorded and the location of the particular CCTV camera, so that the images can be easily located and your identity can be established as the person in the images. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information before processing the request. The Company will respond promptly and in any case within one month of receiving the request.

The Data Privacy Manager will first determine whether disclosure of your images will reveal third party information as you have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the Company is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

7. Covert recording

The Company will only undertake covert recording with the written authorisation of the CEO (or another senior director acting in their absence) where there is good cause to suspect that criminal activity or equivalent malpractice is taking, or is about to take, place and informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection.

Covert monitoring may include both video and audio recording.

Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of particular suspected criminal activity or equivalent malpractice. Once the specific investigation has been completed, covert monitoring will cease.

Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which the Company cannot reasonably be expected to ignore.

8. Staff training

Our operational staff are trained in the use of the CCTV equipment at each site.

9. Implementation

The Company's Data Privacy Manager is responsible for the implementation of and compliance with this policy and the operation of the CCTV system and they will conduct a regular review of the Company's use of CCTV. Any complaints or enquiries about the operation of the Company's CCTV system should be addressed to them.