

## **CCTV Policy**

Kilmac Ltd may use closed circuit television (CCTV) images to provide a safe and secure environment for employees and for visitors to the Company's business premises and on site, such as clients, customers, contractors and suppliers, and to protect the Company's property. This policy sets out the use and management of the CCTV equipment and images in compliance with GDPR and the Information Commissioner's Office CCTV Code of Practice. The Company's CCTV facility records images only. There is no audio recording and therefore conversations are not recorded on CCTV (but see the section on covert recording below).

### **Purposes of CCTV**

The purposes of the Company installing and using CCTV systems include to:

- Assist in the prevention or detection of crime or equivalent malpractice
- Assist in the identification and prosecution of offenders
- Monitor the security of the company's business premises
- Ensure that health and safety rules and company procedures are being complied with
- Assist with the identification of unauthorised actions or unsafe working practices that might result in disciplinary proceedings being instituted against employees and to help in providing relevant evidence
- Promote productivity and efficiency.

### **Location of Cameras**

Cameras can be located at strategic points throughout the Company's business premises and on site, principally at the entrance and exit points. The Company has the right to position 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. No camera focuses, or will focus, on toilets, changing rooms, staff kitchen areas, staff break rooms or private offices. All cameras (with the exception of any that may be temporarily set up for covert recording) are also clearly visible.

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

### **Recording and retention of images**

Images produced by the CCTV equipment are as clear as possible so that they are effective for the purposes for which they are intended. 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 on to, removable media such as CDS 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 a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

### **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 centrally 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.

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 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).

A Director (or another senior director acting in their absence) is the only person who is permitted to authorise disclosure of information 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.

### **Individuals' access rights**

Under GDPR, individuals have the right 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 of your CCTV images, you must make a written request to the Company's GDPR Officer. Your request must include the date and time when the images were recorded and the location of the particular CCTV camera, so that the images can be located and your identity can be established as the person in the images. **Note.** The Company will always check the identity of the employee making the request before processing it.

The HR Officer 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.

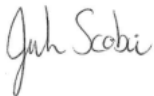
If the Company is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

**Covert recording**

The Company will only undertake covert recording with the written authorisation of a director (or another senior person 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.

A handwritten signature in black ink that reads 'Julie Scobie'.

Julie Scobie  
Financial Director  
2nd May 2023