CCTV Policy

Introduction

The Company uses closed circuit television (CCTV) images to protect the Company's property and to provide a safe and secure environment for employees and visitors to the Company's business premises. This policy sets out the details of how the Company will collect, use and store CCTV images. For more information on your privacy rights associated with the processing of your personal data collected through CCTV images, please refer to the Company's employee privacy notice and data protection policy, or contact the Office Manager.

The Company's CCTV facility, unless there are exceptional circumstances, will only record images. While the Company's CCTV facility is capable of audio recording, only images are recorded and processed.

Purposes of CCTV

The Company has carried out a data protection impact assessment and on the basis of its findings it considers it necessary and proportionate to install and use a CCTV system. The data collected from the system will assist in:

1. Prevention or detection of crime or equivalent malpractice.
2. Identification and prosecution of offenders.
3. Monitoring of the security of the Company's business premises.
4. Ensuring that the Company's health and safety procedures are being complied with.
5. Identification of unauthorised actions or unsafe working practices that might result in disciplinary procedures being instituted against employees and to assist in providing relevant evidence.
6. Promoting productivity and efficiency.

Location of Cameras

Cameras are located at strategic location throughout the Company's premises, including at entrance and exit points and areas of significant employee thoroughfare. 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. No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff kitchen areas, staff break rooms, private offices, or personal domiciles.

All cameras (with the exception of any that may be temporarily be installed for covert recording) are clearly visible, and appropriate signs are displayed prominently so that employees, clients, 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 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 are recorded in constant real-time, 24 hours a day throughout the year.

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, once the hard drive has reached the end of its use, it will be appropriately erased prior to disposal.

Images that are stored on, or transferred on to, removable media such as CDs or which are stored digitally are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of 30 days. However, where a law enforcement agency is investigating a crime, or where the footage is relevant in a disciplinary procedure, 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, to those line managers who are authorised to view them in accordance with the purposes of the system, and other staff who are, permanently or temporarily, authorised to view them by the appropriate line manager or member of staff. Viewing of recorded images will take place in a restricted area to which unauthorised 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:

1. 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.
2. Prosecution agencies, such as the Crown Prosecution Service.
3. Relevant legal representatives.
4. Line managers involved with Company disciplinary and performance management processes.
5. 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 Director of the Company (or another authorised member of the management team 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 for the denial will be recorded.

Individuals' Access Rights

Individuals have the right on request to receive a copy o 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 Office Manager via email. The Company will usually not make a charge for such a request, but we may charge a reasonable fee if you make a request which we judge to be manifestly unfounded or excessive, or for repeated requests. 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.

The Company will usually respond promptly and in any case within one month of receiving a request. However, where a request is complex or numerous the Company may extend the one month to respond by a further two months. Where the Company extends this period, you will be informed in writing before the completion of the initial one month period.

The Company will always check the identity of the employee or visitor making the request before processing it.

The Office Manager will always 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 is aware that covert recording can only be done in exceptional circumstances, for example where the Company suspects criminal activity taking place. On this basis, the Company will only undertake covert monitoring if it has carried out a data protection impact assessment which has addressed the following:

1. The purpose of the covert recording.
2. The necessity of the covert recording.
3. The risks to the privacy rights of the individual(s) affected by the recording.
4. The time parameters for conducting the covert recording.
5. The safeguards and/or security measures that need to be put in place to ensure the covert recording is conducted in accordance with the data protection laws, including the GDPR.

If, after undertaking the data impact assessment, the Company considers there is a proportionate risk of criminal activity, or equivalent malpractice, taking place or about to take place, and if informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection, the Company will covertly record the suspected individual(s). In doing this the Company will rely on the protection of its own legitimate interests as the lawful and justifiable legal basis for carrying out the covert recording.

Before the covert recording commences the Company will ensure that the Director (or another authorised member of the management team acting in their absence) agrees with the findings of the data protection assessment and provides written authorisation to proceed with the covert recording.

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.

Staff Training

The Company will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the laws regulating data protection and privacy with regard to that system.

Implementation

The Director 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 and processing of CCTV images and ensure that at all times it remains compliant with the laws regulating data protection and privacy. Any complaints or enquiries about the operation of the Company's CCTV system should be addressed to the Office Manager.

Data Protection

The Company will process the personal data collected in connection with the operation of the CCTV policy in accordance with its data protection policy, any internal privacy notices in force at the relevant time, and any other relevant information security or data protection policies that the company may from time to time choose to implement. Inappropriate access or disclosure of this data will constitute a data breach and should be reported immediately to the Office Manager in accordance with the company's data protection policy. Reported data breaches may be investigated and may lead to sanctions under the Company's disciplinary procedure.

Last Updated: June 2024