# VIDEO SURVEILLANCE (CCTV) POLICY

## Introduction

The Company uses video surveillance equipment (referred to as CCTV from henceforth) to record images and videos 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 data protection policy.

## 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 may be used to assist in:

- Monitoring of the security of the Company's business premises.
- Prevention or detection of crime.
- Identification and prosecution of offenders.
- Customer / Regulatory requirements
- Ensuring that Health and Safety rules and Company procedures are being complied with.
- Providing relevant evidence for investigations into employee misconduct, or for any of the above situations.

## Location of cameras

Cameras are located at strategic external points throughout the Company's business premises, principally at the entrance and exit points. 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 internally. All cameras are also 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.

## 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, once the 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 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 12 months. 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 managers who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in areas to which other employees will not have access when viewing is occurring.

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.
- 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 Managing Director of the Company 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.

## Individuals' access rights

Under data protection laws, including the General Data Protection Regulation (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 CCTV images relating to you, you must make a written request to the HR Department, details of which are available through the Company's **Data Protection Policy**. 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 is manifestly unfounded or excessive, or is repetitive. 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.

The Company 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.

## 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 Company's Data Protection Officer is responsible for the implementation of and compliance with this policy and for conducting a regular review of the Company's use and processing of CCTV images to ensure that it remains compliant with the laws regulating data protection and privacy. The maintenance, security and operation of the system will be the responsibility of the IT Manager. Any complaints or enquiries about the operation of the Company's CCTV system should be addressed to Company's Data Protection Officer.

## 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. Inappropriate access or disclosure of this data will constitute a data breach and should be reported immediately to the Company's HR Department in accordance with the Company's data protection policy and BOCS-29. Reported data breaches will be investigated and may lead to sanctions under the Company's disciplinary procedure.