



CCTV POLICY

Introduction

New Directions uses closed circuit television (CCTV) images to provide a safe and secure environment for employees and for visitors to the Company's business premises, 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 the Data Protection Act 2018 and the CCTV Code of Practice.

The Company's CCTV facility records images only. There is no audio recording i.e. conversations are not recorded on CCTV (but see the section on covert recording).

Under the Data Protection (Charges and Information) Regulations 2018, individuals and organisations that process personal data need to pay a data protection fee to the Information Commissioner's Office (ICO). New Directions complies with this on an annual basis under ICO Registration: ZA533181

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.
- To assist in the identification and prosecution of offenders.
- To monitor the security of the Company's business premises.
- To ensure that health and safety rules and Company procedures are being complied with.
- To assist with 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.
- To promote productivity and efficiency.

Location of cameras

Cameras are located at strategic points throughout the Company's business premises, this information can be found on the "CCTV location and time period" spreadsheet on the shared drive. Access to this database is limited to selected managers to ensure the entry codes are restricted.

Principally the cameras are located 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, or will focus, on toilets, shower facilities, changing 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 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 suitable 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 a maximum of 15 weeks. Once a hard drive has reached the end of its use, it will be erased prior to their secure disposal.

Images that are stored on, or transferred on to, removable media such as memory sticks or secure folders are erased once the purpose of the recording is no longer relevant. In circumstances where information is required for "ongoing incidents" the incident will be recorded on a list, stating the incident name and who the recording has been shared with. When the Data Protection Champion receives email confirmation that the CCTV recordings are no longer relevant to any investigation they will be deleted from the secure folder. 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 to authorised managers. 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 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 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 is the only person 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. All disclosure requests and their responses will be coordinated and recorded by the Data Protection Champion and Facilities Manager.

Individuals' access rights

Under the General Data Protection Regulations (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 Data Protection Champion (Office Manager). 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 respond promptly and in any case within one month of receiving the request.

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

The Data Protection Champion 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 or removed 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.