CCTV Policy

Introduction

This Policy is based on the Information Commissioners Office (ICO) CCTV Code of Practice and guidelines, in line with the GDPR.

Charles Tennant & Co (NI) Ltd, Tennants Building Products Ltd, Charles Tennants & Co (Cork) Ltd and Walls & Ceilings International Ltd (Tennants) use 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. We also use mobile recording in company vehicles for security, safety and quality purposes.

This policy sets out the use and management of the CCTV equipment and images in compliance with the GDPR and the ICO 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 (also please see the section on covert recording).

The Divisional Manager at each site is responsible for the operation of the CCTV System and for ensuring compliance with this policy and any documented procedures.

Contact details

Airport Road West:	Site Supervisor	+44 (0)28 9045 5135
Herdman Channel Road:	Production Manager	+44 (0)28 9074 0002
Ravenhill Road:	Health & Safety Manager	+44 (0)28 9073 1501
Dublin:	Divisional Director	+353 (0)1 450 3480
Cork:	Divisional Director	+353 (0)21 437 9442
Walls & Ceilings International Ltd:	Logistics manager	+44 (0)1789 763 727

All areas of Tennants operations covered by CCTV fall within this policy. Signs are prominently placed at strategic locations including entrance and exit points to all sites to inform staff, visitors and members of the public that a CCTV installation is in use and who to contact about the system.

Purposes of CCTV

The purposes of the company installing and using CCTV systems include the following (this list is not exhaustive):

- 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 company health and safety rules and 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.
- To enable customer assurance and quality controls.

Location of cameras

Cameras are located at strategic 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, or will focus, on toilets, shower facilities, 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 displayed so that employees, customers and other visitors are aware that 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 per 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 6 months. 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. 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.

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 taking place. 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, 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 Data Controller and those of director level and above are the only people 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. These records will be kept on file at each division.

Individual access rights

In line with the 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 company's Data Protection Officer and the company reserves the right to charge you a fee of £10.00 for the supply of the images requested. 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 40 calendar days of receiving the request.

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

The Data Protection 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.

Third-party processors / accessors

Any third-party that has access to, or processes CCTV data on our behalf will also be subject to this policy and we will have recorded as such.

Covert recording

The company will only undertake covert recording with the written authorisation of the Managing Director (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.

Staff training

All relevant employees will be trained in general awareness of the CCTV system and on the impact of GDPR with regard to that system and how it operated.

In addition, those handling CCTV images or recordings will be trained in the operation and administration of the system to the required degree.

Implementation

The company's Data Protection Officer 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 the relevant division in the first instance, using the contact details given above.

Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.