Contents List:

1 Policy Statement

1.1 This policy sets the Group's position on the use of CCTV in the workplace and its effect on employees, contractors and visitors and other individuals. Governance of CCTV and Surveillance Cameras throughout the Group is the responsibility of the Data Protection Committee (DPC). The DPC may be contacted by emailing dataprotection@ballyvesey.com

2 Purpose and Scope

2.1 The primary uses of CCTV are to assist in the Protection and Safety of Persons, company assets and Property, Prevention or Detection of Criminal Offences and Pursuit of, or Defence of Legal Claims to comply with Chapter 2 Paragraph 1 of Surveillance Camera Code of Practice published by the Home Office (SCCP).

2.2 CCTV camera systems can be seen as intrusive. In considering the potential to interfere with the right to privacy it is important to take account of the fact that peoples' expectations of privacy are both varying and subjective. An individual can, however, rightly expect surveillance to be both necessary and proportionate, with appropriate safeguards in place (Chapter 2 Paragraph 3 SCCP).

2.3 It is not the Group's intended purpose to use CCTV for monitoring the work of employees or finding out whether or not they are complying with the organisation's policies and procedures, to comply with Part 3 of The Employment Practices Code published by the ICO. However, in the course of normal monitoring, where an incident is captured that cannot in good conscience be ignored, the Group, reserve the right to process in the business interests. This may include grievance, or disciplinary proceedings, and defence or litigation of a legal claim.

3 Guiding Principles (SCCP Chapter 2 Paragraph 6)

3.1 System operators should adopt the following 12 guiding principles:

3.1.1 Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

3.1.2 The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3.1.3 There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints. Signs will be displayed prominently to inform employees, contractors, visitors and other individuals that CCTV is in use.

3.1.4 There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

3.1.5 Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

3.1.6 No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

3.1.7 Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

3.1.8 Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

3.1.9 Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

3.1.10 There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

3.1.11 When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

3.1.12 Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

4 CCTV Footage

4.1 Live CCTV footage can only be viewed by: Security Personnel, Directors and Management

4.2 Access may only be approved by the DPC and on an incident by incident basis. Once access is approved by the DPC, recorded CCTV footage can be reviewed (not deleted or amended) by:

- Members of the DPC
- Directors
- Designated Managers
- Statutory bodies such as Police, HSE, once they have made contact with the DPC and submitted a Schedule 2 Request Form to dataprotection@ballyvesey.com as required by the Data Protection Act 2018

4.3 Any other person with interest must obtain authority from the DPC to view recorded footage, providing reasons and justification.

4.4 Any persons whose images are recorded have a right to view those images, and to be provided with a copy of those images, within one month of making a written Subject Access Request (Article 15 GDPR). Availability of images will be subject to the retention period. Individuals making such requests should do so in writing, providing the relevant time and date of the image, so that they may be easily identifiable. The request should be made to dataprotection@ballyvesey.com or by writing to the Data Protection Committee, Ballyvesey Holdings Limited, 607 Antrim Road, Mallusk, Newtownabbey, BT36 4RF.

5 Employees

5.1 As stated, the primary uses of CCTV are to assist in the Protection and Safety of Persons and Property, Prevention or Detection of Criminal Offences and Defence of Legal Claims. However, when CCTV is installed in a workplace, it is likely to capture pictures of employees and workers.

5.2 In accordance with paragraph 2.3 above, CCTV evidence may be used as part of an employee investigation where, in the reasonable belief of management, that there may have been misconduct, or a breach of Health and Safety. In such cases the footage must be requested by the Human Resources Manager and in consideration of any legal implications, its use for this purpose approved by the DPC.

5.3 Where footage is used in disciplinary proceedings, it will be retained by the officiating HR department for a further period of up to five years. The employee will be permitted to see and respond to the images, in addition to their Article 15 right to request a copy, which will be provided within one month.

5.4 Under appropriate circumstances the footage may be provided to Police (or other Competent Authority) with the intention to prosecute for criminal offences. In defence of legal claims, or in pursuance of civil recovery, footage may also be provided to our legal representatives and insurance providers with the intention of providing evidence before the courts. All such disclosure will require the purview and approval of the DPC.

6 Non-Employees

6.1 Where an incident involves a visitor under the instruction of another employer (third party), the relevant employer will be informed of the details. Although the third party may be made aware that there is recorded evidence in the form of CCTV, they cannot be provided with a copy of the footage. A copy of the recorded material can only be requested by the subject themselves. However, the footage can be "viewed only" by the third party by either visiting our premises, or our representative meeting the third party to provide "viewing only" on a portable device.

6.2 As with employees, non-employees, whether under instruction of another employer or not should also note: Under appropriate circumstances the footage may be provided to Police (or other Competent Authority) with the intention to prosecute for criminal offences. In defence of legal claims, or in pursuance of civil recovery, footage may also be provided to our legal representatives and insurance providers with the intention of providing evidence before the courts.

7 Complaints

7.1 Complaints about the operation of the CCTV system should be addressed initially to dataprotection@ballyvesey.com or by writing to the Data Protection Committee, Ballyvesey Holdings Limited, 607 Antrim Road, Mallusk, Newtownabbey, BT36 4RF.

8 Monitoring and Review

8.1 This policy will be reviewed at least annually, or sooner if there is a policy need or legislative change.

8.2 This policy does not form part of employees' terms and conditions of employment and may be subject to change at the discretion of the Data Protection Committee.

Document Control

The Data Protection Committee are the document owner and responsible for ensuring this policy remains current and up to date.

A current version of this document is available to all members of staff on the Security and Governance SharePoint site and is published by the Security and Governance function.

This policy was approved by the Data Protection Committee and is issued on a version controlled basis.

Representative of the DPC signature:  Date: 21/02/2024

Change History Record

Issue	Description of Change	Date of Change
1.0	Initial Issue	
2.0	Review	21/02/2024