

## **CCTV Policy**

This policy provides a framework for the planning, installation, management and maintenance of Closed Circuit Television (CCTV) systems on sites owned or occupied by PFG where there is a building management responsibility

<b><u>Version</u></b>	<b><u>1</u></b>
<b><i>Date Adopted</i></b>	<b>01/06/2022</b>
<b><i>Review Date</i></b>	<b>01/12/2022</b>
<b><i>Expiry Date</i></b>	<b>31/12/2022</b>
<b><i>Target Audience</i></b>	<b>All</b>

At PFG we believe that CCTV plays a legitimate role in helping to maintain a safe and secure environment for all our staff, guests, service users, potential suppliers, employees of its partners and suppliers and contractors. Images recorded by CCTV are Personal Data and as such must be processed in accordance with data protection laws. We are committed to complying with our legal obligations in order to appropriately handle and protect Personal Data and ensure that the legal rights of staff, guests, customers, and potential suppliers, employees of its partners and suppliers and contractors relating to their Personal Data, are recognised and respected.

This policy is intended to enable staff, guests, customers, and potential customers, tenants, employees of its partners and suppliers and contractors to understand how PFG uses CCTV, those responsible for CCTV use, the rights individuals may have in relation to CCTV, who has access to CCTV images and how individuals can raise any queries or concerns they may have.

<b><u>Version Number</u></b>	<b><u>Comments</u></b>
<b>V1</b>	<b>New Document</b>

### 1. Definitions

For the purposes of this policy, the following terms have the following meanings:

CCTV: means cameras, devices or systems including fixed CCTV and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

CCTV Data: means any Data in respect of CCTV, e.g. video images, static pictures, etc.

Data: means any information which is stored electronically or in paper-based filing systems.

**Data Subject:** means any individuals who can be identified directly or indirectly from CCTV Data (or other Data in our possession). Data Subjects include staff, guests, customers, and potential customers, tenants, employees of its partners, suppliers and contractors, and members of the public.

**Data Controller:** is the organisation or authority which, determines how and for what purpose the Personal Data are processed. When operating CCTV, PFG is the relevant Data Controller and is responsible for ensuring compliance with the Data Protection Laws.

**CCTV users:** are those of our employees (or employees of any Data Processors which we appoint) whose work involves processing CCTV Data. This will include those whose duties are to operate CCTV to record, store and retrieve and delete images. Data users must protect the CCTV Data they handle in accordance with this policy.

**Service Provider:** is any organisation that is not a CCTV user (or other employee of a Data Controller) that processes CCTV Data or Personal Data on our behalf and in accordance with our instructions (for example, ADT Fire & Security Solution).

**Data Protection Laws:** means:

a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the “GDPR”) and any equivalent or implementing legislation;

b) all other applicable laws, regulations or court judgements relating to the processing of personal data, data privacy, electronic communications, marketing and/or data security; and

c) any and all legally binding guidelines, recommendations, best practice, opinions, directions, decisions, or codes issued, adopted or approved by the European Commission, the Article 29 Working Party, the European Data Protection Board, the UK’s Information Commissioner’s Office and/or any other supervisory authority or data protection authority from time to time in relation to the processing of personal data, data privacy, electronic communications, marketing and/or data security;

in each case as from time to time in force and as from time to time amended, extended, consolidated, re-enacted, replaced, superseded or in any other way incorporated into law and all orders, regulations, statutes, instruments and/or other subordinate legislation (including the Data Protection Bill 2017 when in force) made under any of the above in any jurisdiction from time to time.

**Processing:** is any activity which involves the use of CCTV Data, whether or not by automated means. It includes collecting, obtaining, recording or holding CCTV Data, or carrying out any operation or set of operations on the CCTV Data including organising, structuring, amending, retrieving, using, disclosing or erasing or destroying it. Processing also includes transferring CCTV Data to third parties.

**Site:** means the PFG premises at PFG, 45 Montrose Avenue, Doncaster and more specifically the Sites listed in Schedule 1 where CCTV is installed.

## 2. About this policy

2.1: We currently use CCTV to ensure our employees are protected in the event of an incident and to monitor the security of the premises and assets contained within (i.e. Tablets/Phones/Personal

Belongings). This policy sets out why we use CCTV, how we will use CCTV and how we will process any CCTV Data recorded by CCTV to ensure that we are compliant with Data Protection Law.

2.2: The images of individuals recorded by CCTV are Personal Data and therefore subject to the Data Protection Laws. PFG is the Data Controller of all CCTV Data captured at our Site.

2.3: This policy covers all staff, guests, customers, and potential suppliers, employees of its partners and suppliers and contractors and may also be relevant to members of the public visiting the Site.

### 3. Staff responsible

PFG Kelly Hicks has overall responsibility for ensuring compliance with Data Protection Laws and the effective operation of this policy. Should you have any queries on the use of CCTV or surveillance systems by us please contact Mark Gibson

### 4. Why we use CCTV

4.1: We currently use CCTV around our Site as outlined below. We believe that such use is necessary for the following legitimate business purposes:

(a) to prevent or detect crime and protect buildings and assets from damage, disruption, theft, vandalism and other crime;

(b) for the personal safety of staff, guests, customers, and potential customers, tenants, employees of its partners, suppliers and contractors and other members of the public and to act as a deterrent against crime;

(c) for health and safety of those supporting our service users;

(d) to support law enforcement bodies in the prevention, detection and prosecution of crime

We may implement or use CCTV for purposes other than those specified above which we will notify you of from time to time.

### 5. MONITORING

5.1: The locations of the CCTV are chosen to minimise the viewing of spaces/individuals which are not relevant to the legitimate purpose of the monitoring as specified above.

5.2: Currently, none of our CCTV records sound.

5.3: A recorded feed can be accessed and images are only revisited in the event of an incident or if a request is made.

5.4: Any staff using CCTV will be given training to ensure that they understand and observe the legal requirements relating to the processing of any Data gathered.

### 6. How we operate CCTV

6.1: Where CCTV is in use at our Site, we will ensure that signs are displayed at the entrance of the surveillance zone to alert staff, guests, customers, and potential customers, tenants, employees of its partners, suppliers and contractors that their image may be recorded. The signs will contain details of the organisation operating the system (where they are operated by a third party) and who to contact for further information.

6.2: We will ensure that live feeds from the CCTV are only viewed by appropriately authorised members of staff or third-party service providers whose role requires them to have access to such CCTV Data. Recorded images will only ever be viewed in the Head Office or the General Manager's Office which are secure and restricted areas by our staff, centre managers and the Health and Safety Manager.

### 7. How we use the Data

7.1: In order to ensure that the rights of individuals recorded by our CCTV are protected, we will ensure that CCTV Data gathered from such systems is stored in a way that maintains its integrity and security. This may include encrypting the Data, where it is possible to do so.

7.2: We will ensure that any CCTV Data is only used for the purposes specified in section 4.1 above. We will not use CCTV Data for another purpose unless permitted by Data Protection Laws.

7.3: Where we engage Data Processors to process Data on our behalf, we will ensure contractual safeguards are in place to protect the security and integrity of the Data.

## 8. Retention and erasure of Data

8.1: Data recorded by our CCTV will be stored locally on a cloud server accessible by our site. We will not retain this Data indefinitely but will permanently delete it once there is no reason to retain the recorded information. Exactly how long the Data will be retained for will vary according to the purpose for which it was recorded. For example, where images are being recorded for crime prevention purposes, CCTV Data will be kept only for as long as it takes to establish that a crime has been committed, the images will be kept until the process is completed. In all other cases, recorded images will be kept for no longer than 30 days before being overwritten and permanently deleted.

8.2: At the end of its useful life and in any event within 7 years all Data stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs or hard copy photographs will be promptly disposed of as confidential waste.

## 9 Ongoing review of our use of CCTV

9.1: We will periodically review our ongoing use of existing CCTV at our Site to ensure that its use remains necessary and appropriate and in compliance with Data Protection Laws.

9.2: We will also carry out checks to ensure that this policy is being followed by all staff.

## 10. Rights of Data Subjects

10.1 As CCTV Data will identify individuals, it will be considered Personal Data under applicable Data Protection Laws. Under Data Protection Laws, Data Subjects have certain rights in relation to the Personal Data concerning them. These are as follows:

(a) the right to access a copy of that Personal Data and the following information (this may include CCTV Data captured by our CCTV):

(i) the purpose of the processing;

(ii) the types of Personal Data concerned;

(iii) to whom the Personal Data has or will be disclosed; and

(iv) the envisaged period that the Personal Data will be stored, or if not possible, the criteria used to decide that period;

(b) the right to request any inaccurate Personal Data that we hold concerning them is rectified, this includes having incomplete Personal Data completed;

(c) the right to request the Personal Data we hold concerning them is erased without undue delay, where it is no longer necessary for us to retain it in relation to the purposes it was collected;

(d) the right to request restriction of our processing of Personal Data in certain circumstances; and

(e) the right to lodge a complaint with the Information Commissioner's Office, if the Data Subject considers that our processing of the Personal Data relating to him or her infringes Data Protection Laws.

## 11. SERVICE PROVIDERS

11.1 In order to operate CCTV across our Site we appoint service providers to provide us with maintenance services related to that CCTV. Such service providers act only on our instructions and on our behalf for the purposes listed in section 4.1 above. We require these service providers by contract to safeguard the privacy and security of Personal Data they process on our behalf.

## 12. Requests of disclosure by third parties

12.1: No images from our CCTV cameras will be disclosed to any third party (other than our third-party CCTV maintenance service providers Choice Fire and Security Solution), without express permission being given by The General Manager Data will only be disclosed to a third party in accordance with Data Protection Laws.

12.2: In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

## 13. Complaints

13.1: If any member of staff has questions about this policy or any concerns about our use of CCTV, then they should speak to Martin Smith in the first instance.

13.2: Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure. If you are not an employee, you can use our official complaints procedure.