PRIMA GROUP

CCTV Policy

Contents

CCTV Policy

1 Aim of the Policy

This policy has been drafted with reference to the ICO website and the Amended Surveillance Camera Code of Practice

In order to be compliant with UK GDPR (United Kingdom General Data Protection Regulation), organisations need to make sure that Closed-Circuit Television (CCTV) is really the right option, establish why it is needed and whether there are any other less intrusive options that could be explored.

If the decision is taken to use CCTV, then a document is required to support this, detailing how CCTV will be used, why it is being used, how long the recordings will be kept, how the recordings will be kept secure and the responsibilities of employees in relation to CCTV. This could include limiting access to the CCTV to a few key employees.

Signs will need to be in place so that people know they are being recorded. The signs need to be clear and obvious, telling people that CCTV is in operation.

2 Who does this Policy apply to?

This policy applies to all employees. An audit has been undertaken on existing CCTV in operation on properties within the Prima Group's ownership or management and the information is recorded in the **CCTV Log.** A Data Privacy Impact Assessment (DPIA) has also been undertaken to assess the risk in general across all locations where Prima Group has CCTV surveillance in use. This is therefore not required to be undertaken for additional sites.

However, the **CCTV checklist at Appendix 1** should be considered and completed before the installation of CCTV at any additional proposed locations. This is a precursor to completing the CCTV Log form on SharePoint **CCTV Log form.** Regular review of the requirement to retain CCTV at these sites will be required to be undertaken. Any queries regarding this should be directed to risk@primagroup.org

3 Reasoning on decision to use CCTV

Prima Group currently only has CCTV surveillance in operation at 6 of their managed and/or owned sites.

UK GDPR responsibility on one of these sites (45-46A Dovecot Place) has been negated. This is because Prima Group is not the data controller and does not process any of the information captured there either.

The remaining sites are listed below with the reason(s) why the Prima Group feels that

CCTV is the right option for these locations:

Site	Why CCTV is needed
Jericho Court	Sheltered scheme – safety and wellbeing of residents
Maud Roberts Court	Sheltered scheme – safety and wellbeing of residents
Chestnut Court	Sheltered scheme – safety and wellbeing of residents
72/74 Stanley Road	Retail/office unit – for the safety and security of the premises
15-16A Dovecot Place	Monitoring the upkeep and maintenance of the building
Leasowe Community Hub, 236 Twickenham Drive	Prima Group office – to detect crime – area around the shops has a history of ASB

In addition, to assist in the management of anti-social behaviour, Prima Group has more recently invested in 5 cloud based CCTV systems which will be installed at various locations for set periods of time. The CCTV log will be updated accordingly with up to date information on each location.

4 How the recordings will be kept secure and how long we will keep them for

There are legal and regulatory requirements for housing associations to adhere to when retaining, or disposing of, data about their tenants, applicants for housing, suppliers, employees, agents, volunteers and board members. Disposal is as important an issue as retention: premature disposal can mean the loss of information that is critically required, while retaining data can expose organisations to risk as well as be a cost to their business.

The minimum statutory retention period is, "*the minimum time necessary*", and the National Housing Federation's minimum recommended retention period is 30 days.

Prima Group has set retention levels on CCTV recordings at each of the relevant sites as outlined in the **CCTV Log**.

5 Responsibilities of employees in relation to CCTV

Establishing a clear basis for the processing of any personal information is essential, and the handling of information relating to individuals collected from surveillance systems is no different.

Viewing of live images on monitors should usually be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location. Recorded images should also be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to authorised persons, or it may be more appropriate to only view recorded images after an incident has occurred.

Access to footage at each of the sites with CCTV, where we have GDPR responsibility is detailed below as outlined in the **CCTV Log**.

6 Signage

All schemes with CCTV will have signage so that people know they are being recorded. The signs need to be clear and obvious, telling people that CCTV is in operation. The sites for which Prima currently has UK GDPR responsibility in this regard have signage as outlined in the **CCTV Log**.

7 Using drones with cameras

Prima Group currently uses a drone with a camera to film sites and buildings. This is currently operated by the Communications and Marketing Advisor.

The operator ensures that the drone is in sight at all times and stays below 400ft, does not fly the drone over a congested area, never flies within 50 metres of a person, vehicle or building not under Prima Group's control, and ensures any images obtained using the drone do not break privacy laws.

The operator will always consider their surroundings, apply common sense and may need to let people know before recording starts.

The operator will remain clearly visible so it will be easier for members of the public to know they are the person responsible for the drone and use signage and/or wear a hi-vis vest. The images will be kept safe and if they are not necessary, they will be disposed of appropriately. This is because, individuals may not always be directly identifiable from the footage captured by the drone, but can still be identified through the context they are captured in or by using the device's ability to zoom in on a specific person.

It is important that the recording system on the drone can be switched on and off when appropriate. This is particularly important given the potential for the cameras to capture large numbers of individuals from a significant height. Unless there is a strong justification for doing so, and it is necessary and proportionate, recording should not be continuous.

8 Making sure we do what we say

This policy will be reviewed as and when needed but generally every 2 years.

In accordance with the CCTV checklist, those officers responsible for each site will ensure the relevant employees have received training on how to operate and manage CCTV systems.

8.1 Access to CCTV

The release of recorded footage will be allowed to law enforcement in order to aid an investigation on the approval of the Risk and Assurance Officer. Any such request must be directed to risk@primagroup.org and be valid and lawful.

Images will not be routinely disclosed to other third parties, without express permission being given by the Risk and Assurance Officer who will ensure the disclosure meets with UK GDPR.

The Risk and Assurance Officer will maintain a log of all disclosures of CCTV images. No images from the CCTV system or recordings in any format shall be posted online or disclosed to the media.

8.2 Subject Access Requests

Data subjects may make a request for disclosure of their personal information and this may include CCTV images (data subject access request). In accordance with Prima's Subject Access Request procedure, images of third parties may be obscured when disclosing CCTV data, when it is considered necessary to do so.

9 Other things to consider

9.1 Prima policies and procedures

This policy should be read together with:

- Data Protection Policy.
- Privacy Statement.
- Subject Access Request Procedure.

9.2 Legislation and Guidance

A number of pieces of legislation and guidance have informed this policy including:

- ICO guidance.
- UK GDPR.
- Amended Surveillance Camera Code of Practice.
- Civil Aviation Authority CAP2320 Drone and Model Aircraft Code.

10 Consultation

This policy has been consulted on with employees and contractors on how we are currently using CCTV and image recordings between the period February 2023 to December 2023. The consultation was mostly centred around updating the CCTV log. It is a requirement of data protection law for an organisation to have the following appropriate measures in place if using CCTV or video surveillance.

- tell people they may be recorded, usually by displaying signs, which must be clearly visible and readable
- control who can see the recordings
- make sure the system is only used for the purpose it was intended for - for example, if it was set up to detect crime, it must not be used to monitor how much work employees do

The ICO also publishes guidance about UK GDPR and the use of CCTV and this policy is aligned with that guidance.

11 Equality Impact Assessment

Prima welcomes feedback on this policy and the way it operates. We are interested to know of any possible or actual adverse impact that this policy may have on any groups in respect of gender or marital status, race, disability, sexual orientation, religion or belief, age or other characteristics.

The policy has been screened to determine equality relevance for the following equality groups: gender or marital status, race, disability, maternity or pregnancy, sex, sexual orientation, religion or belief, age or other characteristics.

12 Data Protection

Personal data that is inappropriately accessed or disclosed may constitute a data breach. The UK GDPR (United Kingdom General Data Protection Regulation) requires organisations to keep a record of all data breaches and, where the breach is likely to result in a risk to the rights and freedoms of individuals, the organisation must notify the Information Commissioner within 72 hours of becoming aware of the breach. If the data breach results in a high risk to the rights and freedoms of individuals, those individuals must be notified without undue delay.

13 Document Control Data

Version:	V32024
Review Date:	December 2023
Name of Reviewer:	Julie Hunter – Risk and Assurance Officer
Owner of the policy:	Director of Insight and Group Services
Consultation Panel:	Insert the titles of those who have been consulted
Change Log:	Page 3 and 4 – Sites where we have CCTV installed updated Page 5 – updated to review every 2 years Page 6 – amendment - third party data *may* be

	obscured Page 6 and 7 - consultation
Date approved by EMT:	12 February 2024
Date to Customer Voice Board:	N/A
Date approved by Committee:	N/A
Date approved by Group Board:	N/A Policy delegated by Board to EMT for approval
Date of Equality Impact Assessment:	19/12/2023
Date due for next review:	February 2026

Appendix 1 – CCTV Checklist

CCTV imagery is considered personal data under UK GDPR and requires the same data protection level of consideration.

We (Prima Group) have considered the need for using CCTV at specific locations and have decided it is necessary for protecting the safety of individuals, or the security of premises. We will not use the system for any incompatible purposes and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate.

	Yes/No	Who/What/Where/How
There is a named individual who is responsible for the operation of the system located at ……		
Prior to processing we have clearly defined the problem we are trying to address.		
We have identified and documented an appropriate lawful basis for using the system, taking into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018.		
Our system produces clear images which we can easily disclose to authorised third parties. For example, when law enforcement bodies (usually the police) require access to investigate a crime.		
We have positioned cameras in a way to avoid any unintentional capture of private land or individuals not visiting the premises.		
There are visible signs showing that CCTV is in operation. Contact details are displayed on the sign(s) if it is not obvious who is responsible for the system.		
We securely store images from this system for a defined period and only a limited number of authorised individuals may have access to them.		
We are able to access recordings/images to enable us to respond to individuals making requests for copies of their own images, or for images to be erased or restricted.		