



CCTV Policy

Policy details	
Name of policy: CCTV Policy	Author name: Kasandra Silcott
Date of Issue: 26 March 2022	Department: All within RHP Group
Date for review: 12 April 2025	No. of pages: 9
Approved by: Leadership Team	

Statement of intent

Closed-circuit television (CCTV) is the use of cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on a suitable platform.

This policy sets out how the group will use and manage CCTV equipment and image compliance with the Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 ('the GDPR'), as well as the ICO CCTV Code of Practice.

This policy covers RHP Group and all subsidiaries within the group, who are known throughout this policy as 'the group'.

This policy applies to all staff (including temporary, casual or agency), contractors, consultants, suppliers, and data processors working for, or on behalf of the group and should be applied by the above in relation to our customers. The installation and use of CCTV by our customers is also covered.

The group uses CCTV both internally and externally, to help:

- Provide a safe, secure working environment for employees and visitors to our business premises
- Provide a safe, secure living environment for our retirement schemes and across communities when and where appropriate
- Assist in the identification and prosecution of offenders
- Ensure that health and safety rules and company procedures are being complied with



CCTV Policy

- 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
- Assist with the identification of breaches of our tenancy agreement which might result in enforcement action

Closed Circuit Television Systems (CCTVS) are installed at various sites across the group. The CCTV Register can be found:

RHP- [\[Insert link to CCTV Register\]](#)

Coop - [W:\GOVERNANCE CHS & CO-OPS\CCTV working group\CCTV REGISTER.xlsx](#)

Cameras within the group's business premises are located at strategic points, primarily at the entrance and exit points. They are positioned to only cover communal areas. No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff kitchen areas, staff break rooms or private offices.

The group will meet the guidance set out in the Information Commissioner's Office (ICO) "CCTV code of practice" relating to the recording of sound. This states that only in exceptional circumstances should conversations be recorded and where audio equipment is supplied with a sound recording facility, this should be turned off or disabled. The group will therefore not generally record sound and do so only where the circumstances meet the requirements of 'exceptional circumstances' as set out in the "ICO CCTV code of practice".

Appropriate signs are displayed so that employees, customers, visitors, and members of the public are aware they are entering an area covered by CCTV.

The group recognises that our customers may wish to install their own CCTV system within the private dwellings they rent from us. Whilst we cannot regulate these systems, we encourage compatibility with the provisions of this policy.

Relevance

The Data Protection Act 2018 [UK GDPR] and The General Data Protection Regulation 2016/679 (EU GDPR) requires the processing of personal data to be lawful, fair, and transparent. As CCTV collects personal data its usage is governed by these laws.



CCTV Policy

The group must identify their lawful basis for using or permitting the use of CCTV. In almost all cases, business owners can rely on legitimate interests or the need to comply with another legal requirement for this purpose. However, we must justify this against the area of coverage provided by the camera. Data subject's rights and freedoms cannot be overridden, especially in the case of legitimate interests. Even inside a work premises, employees have a right to privacy.

The group's CCTV installations include several workplace locations. Where images captured on CCTV support allegations or reveal evidence of gross misconduct, the group reserves the right to use these images in bringing a disciplinary case against an employee for gross misconduct.

Covertly recording colleagues and customers without their permission is likely to be unlawful data processing and potentially a criminal offence. The group will only ever use covert recording where the legitimate interests of the recorder outweigh the interests of those individuals being recorded.

Data subjects are entitled to understand when their personal data is being processed; therefore, we must be transparent in our use of CCTV. We will ensure that CCTV cameras are visible and communicated via signage, with the signage indicating the areas covered and instructions for further information

It is important to highlight that some uses of CCTV are not covered by the Data Protection Act e.g., the use of cameras for limited household purposes (such as to protect a home from a burglary) even if the camera overlooks the street. Images captured for recreational purposes, such as with a mobile phone, digital camera or camcorders are also exempt.

If CCTV is not utilised in line with the Data Protection Act 2018, the Information Commissioner can investigate and enforce these rules issuing fines where appropriate. For more information on Data Protection please see our Data Protection Policy.

Article 8 of the Human Rights Act 1998 makes provisions for the right to family and private life. This means that an individual has the right to the level of personal privacy. Interference with an individual's Article 8 right to privacy is permitted if there are legal justifications. Anyone using CCTV must balance the benefits of using CCTV against an individual's right to privacy.

The Regulator for Social Housing, Homes and Community Standard, gives clear responsibility to the group, as a social landlord to keep neighbourhoods and communal areas safe and to tackle anti-social behaviour within those neighbourhoods. CCTV is a facility commonly used to help the group to meet this regulatory requirement.

Guiding Principles

When considering the use of CCTV, the group will ensure that we have considered the following:

➤ **Assessment of the need**

An initial assessment will be carried out to determine the objectives of each installation of a CCTV system. This is because the effect CCTV systems could have on individuals' privacy must be measured against these objectives.

The extent of assessment will depend on the size of the proposed office, scheme or residential area and the level of impact it is likely to have on people's privacy. The assessment should also consider factors such as the likely cost of the scheme and whether planning may be required.

The assessment should also consider legislative requirement, clearly documenting our legal purpose

➤ **Assessment of location of the CCTV cameras**

When setting up new CCTV cameras, the group's staff and contractors who install CCTV on behalf of the group should ensure that:

- ✓ All cameras are in a noticeable position within public and/or staff view and must not face directly into a customers' property. Signs will be erected to ensure staff, customers, visitors and/or members of the public are aware that they are entering an area that is covered by CCTV. The signs will include the RHP logo and the relevant contact details for accessing the footage.
- ✓ Once installed, all equipment including cameras must be audited, ensuring that only the designated areas are monitored, and high-quality pictures are available in live and playback mode.

➤ **Training**

CCTV equipment will be available only to staff who have been adequately trained. Minimum training requirements will include technical knowledge enough to operate the equipment along with an understanding of the implications of Data Protection and Human Rights Legislation. All staff will have access to the Information Commissioner's Office "CCTV code of practice". Members of staff who have undergone training may conduct in-house training.

➤ **Review and Maintenance**

All CCTV equipment should be audited, on an annual basis. Should the audit flag any remedial work, these works will be completed within 6 months of becoming aware there is an issue.

The use of corporate CCTV units will be reviewed at least annually by the Data Protection Officer to ensure that they comply with legal obligations and the "CCTV code of practice", as well as reviewing its effectiveness. The Data Protection Officer will keep a written record of those reviews.

➤ **Storage and access to recordings**

Recorded images will be securely stored on digital video recorders (DVRs) or secure cloud-based storage. Recorded images will be stored for a maximum of 30 days unless the information relates to an ongoing investigation or legal case.

Where this is the case, we'll erase the images and audio recordings, within three months of closing the ASB case or any legal proceedings concluding. This follows the data protection principles.

Access to recorded images will be strictly restricted. Any internal request for access or use of CCTV images and all viewing arrangements - including from other staff members must be overseen by the Resolutions Team within RHP and Business Services Manager within coop.

The Group will make available CCTV footage when requested (on DVD or other suitable means) to:

- ✓ law enforcement agencies, where it is believed that the images will assist in a legal enquiry
- ✓ prosecuting agencies such as the Crown Prosecution Service
- ✓ legal representatives such as lawyers
- ✓ the media, where a decision has been made by the police that the footage is needed to assist in identification of the perpetrator of a criminal incident (the wishes of the victim will be considered)
- ✓ fulfil the requirements of a subject access request by an individual, including employees
- ✓ insurance agencies where the request is reasonable and appropriate given the circumstances – the guidance of the Data Protection Officer should be sought.

Where the group is statutorily required to share CCTV recordings with third parties such as the Police, the Data Protection Officer (or a manager with direct responsibility for CCTV) must authorise the granting of the request, and a written record of any such disclosures will be kept.

Where an individual makes a request to view images of themselves, the group will follow the requirements of the "CCTV code of practice" in providing the images. An individual making a request will need to do so in writing or via an appropriate form. When a request is made, the Data Protection Officer (or a manager with direct

responsibility for CCTV) must authorise the granting of the request, and a written record of any such disclosures will be kept.

In line with the Data Protection Act 2018, data subjects have a right of access to information held about them, which could result in the need to disclose CCTV footage (as mentioned above). When disclosing footage for this purpose, the group will ensure that only footage containing the requester is disclosed and that in doing so we are not disclosing the personal information of any other data subject. This may involve blurring parts of the footage such as figures or license plates.

Some door entry systems have inbuilt cameras to allow for greater security within the building. The group will treat the images captured by these cameras in the same way as images captured by CCTV cameras.

➤ **Requests for permission to install CCTV or a camera doorbell in our properties**

Customers who wish to use CCTV cameras or a camera doorbell at their home must apply to RHP for permission, in writing, before installation. The Director of Housing Services and Head of Housing Services within RHP and Business Services Manager within coop will be responsible for processing such applications; taking pro-active steps to check and re-iterate that the CCTV camera(s) or a camera doorbell must capture only the resident's property. They will not be permitted to capture other customers' property, communal areas, or public spaces.

Customers who have permission to install a CCTV system should ensure it captures only images within the boundary of the private domestic property (including their garden), if the system captures images of people outside the boundary of the private domestic property, for example, in neighbours' homes or gardens, shared spaces, or on a public footpath or a street, then the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) will apply, and they will need to ensure the use of CCTV complies with these laws.

The application process can be supported by the Data Protection Officer if necessary.

Failure to meet the legal requirements of CCTV may be a breach of a customers' tenancy agreement and RHP may ask for the removal the CCTV equipment or doorbell.

Should a customer mis-use CCTV or it becomes a factor within a breach of tenancy or anti-social behaviour case, the group reserves the right to request that cameras are removed. If reasonable and proportionate, tenancy enforcement action may be taken. Guidance may be sought from the Data Protection Officer or a legal representative.

A copy of this Policy will be provided to customers on request and will be publish on our website.

Connected Documents

Data Protection Policy
HR Data Protection Policy
Document Retention Policy
Subject Access Request Policy
ICO CCTV Code of Guidance
Closed-circuit television (CCTV) Register
CCTV Request Form
CCTV Factsheet

Explicit exclusions

This policy only covers RHP Group CCTV equipment and although it provides guidance for customer's personal equipment such equipment is not directly covered under this policy.

Definitions

1. CCTV - Closed Circuit Television Systems
2. The group - All businesses operating within RHP group
3. Data Subject - an identifiable natural person who can be identified, directly or indirectly by the CCTV.

Responsibilities

➤ Data Protection

In applying this policy, all members of staff must comply with the group's Data Protection Policy and ensure that the personal information supplied by customers is protected at all times.

Staff found abusing the CCTV system may be subject to disciplinary action in accordance with the Disciplinary Policy.

➤ Information Commissioner's Office

Because the information captured by CCTV can be used for crime prevention, the group is required to notify the Information Commissioner's Office that it is a data controller and pay the relevant registration fee. The notification includes the purposes for which the images are used, the disclosures that are made and other relevant details. The group will meet this requirement and renew the notification when due.

➤ **Equality and diversity**

The group is aware of its obligations under the Equality Act 2010. The group will apply this policy consistently and fairly and will not use CCTV to discriminate against anyone.

The group will ensure this policy is accessible and will agree with individuals how best to meet their accessibility requirements when the policy is requested.

➤ **Safeguarding**

The group takes its responsibility towards the safety of staff, customers, and visitors seriously. As part of our safeguarding obligations CCTV can be used:

- ✓ As a proactive approach to safeguard people and protect property
- ✓ To provide as required, any evidence of activities to support safeguarding enquiries and or referrals.

Procedures for implementation

Policy to be rolled out via team huddles once it has been approved.

Measure of Success

What targets have you set to measure the success of the policy in meeting its objectives, how and when will you review its progress.

CCTV being managed in line with the policy, team who process CCTV will be audited against the requirements of the policy.

This policy will be reviewed at least every 3 years, or as required following changes to the business or any associated processes. The Data Protection Officer and the Head of Housing Services is responsible for ensuring completion of the policy reviews.