CCTV Policy

DESIGN HEADER TO INCLUDE POLICY NAME AND DATE RANGE

INFORMATION

Policy Name	**CCTV Policy**
Effective Date(s)	**May 2024**
Approved By	**Risk & Compliance Group**
Approval Date	**21st May 2024**
Policy Owner/Dept	**Data Protection Lead**
Policy Author	**Data Protection Lead – Laura Hughes**
Review Date	**May 2026**
Policy Framework Ref	**DP3**
Version Number	**3.0**

Version Control

Version	Date	Changes	Approver
3.0	April 2024	6.2.4 Update to wording regarding footage download Link to documents &online forms updated **Appendix 1 – CCTV Viewing and Download Process** **Appendix 2 – Access Log (Police)** **Appendix 3 – Access Log (Staff)** **Appendix 4 – CCTV Download Request** **Appendix 5 – CCTV Review Form**	

Your Housing Group Strategic Priorities			
Safe	☒	Viability	☐
Landlord	☐	Growth	☐
People	☐	Technology	☐

Relevant National Standards or Regulation	Please State if the Policy aligns to any of the Regulators Standards: • Governance and Financial Viability Standard • Neighbourhood and Community Standard

Relevant Legislation	Please list any legislation applicable to the Policy • The Data Protection Act 2018, • The Protection of Freedoms Act 2012

	• Information Commissioner's Office ("ICO") Code of Practice for Surveillance Cameras and Personal Information • The Home Office Surveillance Camera Code of Practice • The UK General Data Protection Regulations

1. Purpose of the Policy

This policy is designed to offer guidance on how we use, check and operate CCTV across YHG. It also outlines the procedure for obtaining copies of CCTV and disclosure of the same outside YHG

2. Scope of the Policy

a. This policy applies to all staff of the Group who manage the implementation of CCTV systems, oversee the operational maintenance and maintenance contracts for CCTV.

b. This policy also applies to anyone operating CCTV systems either on an active day-by-day basis or purely for the purposes of reviewing and retrieving recorded activity, on those CCTV systems.

2.3 This policy applies to external suppliers who supply, maintain, operate and remove CCTV systems on behalf of the Group acting as a 'Data Processor'.

2.4 This policy will cover all the Group sites, where CCTV is already implemented and sites where CCTV is proposed for implementation. It will not cover sites where CCTV is controlled (installed, managed and/or operated) by another company or organisation designated as 'Data Controller' for that system, unless they are contracted as a 'Data Processor' by the Group.

2.5 The Group does not use General Covert CCTV

2.6 There may be advances in technology or proposed use of equipment by the Group which is not being used at the time of writing this Policy such as: unmanned aerial systems, automatic number plate recognition, body worn video, biometric characteristic recognition or facial recognition etc. Where use of this type of technology is being considered, staff must complete a Data Privacy Impact Assessment (DPIA) with the support of the Data Protection Lead and any other relevant officers in order to consider proportionality and legal justification for such use. Further discussion and approval may also be required from the Risk and Compliance Group.

2.7 This policy will cover: -

i. the Groups use of Overt CCTV,
ii. requests by YHG staff to view CCTV footage, and
iii. requests by external organisation, agencies or individuals to view CCTV including out of hours requests to view CCTV by the police

2.8 This policy will not cover: -

i. Directed Covert CCTV by YHG or other third parties on the Groups behalf,
ii. personal CCTV in the individual properties we let, held and managed for the purposes of our tenants own personal use. Any such footage disclosed to the Group by the 'controller' (the controller being the owner/operator of the system), from that CCTV System, would fall under the Data Protection Policy. Any requests for the installation

of CCTV by a tenant should be dealt with in the same way as any request for consent to an alteration/addition to a property and referred to the relevant Property Agent for consideration who may also direct the tenant to the Information Commissioners Office for further guidance on use of CCTV.

3. Definitions

Overt CCTV: Overt surveillance is carried out with the full knowledge of staff, residents and the public, whose images are captured using the system. The cameras are on open display and there are signs around the building advertising their use. This is a common method of deterring vandalism theft or anti-social behaviour. The images may be retrieved should an incident occur, as an aid to the identification of the perpetrator and subsequent action. On-going observation of the CCTV images may be required, to ensure ongoing safety of individuals where there is a legitimate purpose to do so.

Covert CCTV (or General Covert CCTV): Covert surveillance is when the cameras are not advertised and are hidden from view. Images are captured without the knowledge of residents or the public and are usually monitored as an ongoing process.

Directed Covert CCTV: Directed covert surveillance, is when a camera is secretly put in place and hidden from view. There are no signs displayed to inform the residents or local people that cameras are in operation, so as not to prejudice the purpose of the camera's installation. It is usually carried out in response to a serious or ongoing problem of criminal or anti-social behaviour (ASB) activity. In this case, cameras are installed for a fixed period of time, as an attempt to gather evidence. The images will be monitored at the end of the fixed period, to see if evidence of the ASB or criminal activity has been captured.

Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

4. Consultation

This policy has been approved by Risk & Compliance Group.

5. Background and Context

This policy has been reviewed in response to a review of process requested by the Ombudsman, as part of the update and checking procedure a whole policy review has been completed. It sets out the context for the use and monitoring of Overt CCTV across the Group and complies with relevant legislation.

6. Policy Detail

6.1 Operational Requirements

All current and any proposed CCTV systems will comply with the 12 principles of the Surveillance Camera Code of Practice through the following actions:

6.1.1 All CCTV systems will have a documented specific purpose, which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

6.1.2 All CCTV systems will have an affiliated Data Privacy Impact Assessment, which must be put in place before a new system is implemented and will be reviewed annually.

6.1.3 All CCTV systems will have signage defining who is operating the CCTV system, including a contact point for access to information and complaints together with the purpose for the CCTV system.

6.1.4 All CCTV systems will have a defined manager, usually the relevant scheme or building manager, with those roles and related tasks and responsibilities clearly defined. They will operate under the direction and control of the relevant Director in line with this policy.

6.1.5 This Policy (and any others + guidance) will be approved after consideration at Risk & Compliance Group. They will be available to staff via our intranet system, Youggle. Where necessary they will be available to tenants via notices in schemes and the YHG website.

6.1.6 CCTV is included within YHGs retention Policy and associated schedule. CCTV will only be kept outside of the maximum period stipulated where it is required for legal, insurance or other specified purposes. It will be destroyed in line with those retention times if so kept.

6.1.7 There will be defined procedures regarding Data Disclosure to external organisations/persons as set out in 'Subject Access Request' or 'Third Party Disclosure' and disclosure within YHG as set out in 'Internal Group requests for access to CCTV' appended to this policy:

a. All instances of internal or external data disclosure must be raised with the DP Lead and a record of the disclosure recorded, in-line with the above procedures.

b. Internal access to CCTV footage may be accessible other than as set out above only if agreed with the DP Lead that staff members are authorised for the purpose of this Policy in conjunction with the Chief Operating Officer, Director of Customer Service Delivery and/or Director of Customer Contact & Experience as appropriate and documented in any DPIA or CCTV checklist.

6.1.8 CCTV images and/or data, including but not limited to recorded video, will not be held on the CCTV system for longer than it is required for the stated purpose, to enable action and/or retrieval in respect to any requests. This is a period no longer than 30 days.

6.1.9 Extracted CCTV images and/or data on removable media, must be held according to the Groups retention schedule and the retrieval of CCTV appendices to this policy, stored securely to prevent accidental loss or theft and also if required for future references if required for a legal case.

6.1.10 CCTV systems equipment (recorders, displays and cameras) are to be kept secure to prevent tampering, damage or destruction of data or illegitimate disclosure of data. This is to ensure the adequacy of the data:

a. Cameras should be placed to ensure they are free of obstructions. Consideration should be given to seasonal elements such as tree growth etc. to ensure ongoing adequacy of the footage.
b. Where feasible cameras should not be easily accessible for tampering with and where necessary security measures, such as protective covering put in place
c. CCTV display screens should not be openly visible to the public, residents of schemes or tenants.
d. Where CCTV display screens are actively monitored, access and visibility to the screen(s) should be limited and secured as best as possible. Signage should inform Data Subjects where any CCTV is actively monitored.

6.1.11 Only authorised Group staff have access to CCTV systems and all staff should ensure the legitimacy of external support and maintenance staff who are granted access to the CCTV system(s).

6.1.12 Appropriate inductions and training will be provided to all authorised Group staff who deal with the CCTV systems. This includes communication of relevant policies and procedures. There will be training delivered following approval of this policy to all relevant groups.

6.1.13 CCTV systems should be maintained to check they are in operational order:
a. The appointed contractor or scheme manager will advise if there are any maintenance issues with installed CCTV and repairs will be undertaken on notice of a deficiency to ensure CCTV is operational.

6.1.14 Regular reviews should be made to ensure the effectiveness, validity and quality of the systems, ensuring all cameras are operational and recordings and their related metadata are valid (e.g. date and time stamps, camera position or name, etc.);
a. Annual reviews of CCTV will be undertaken by scheme managers or equivalent. These will use the form in Appendix 5 of this policy

6.1.15 A record should be maintained of all actions carried out against the CCTV system, whether maintenance, support tasks or data retrieval. Appendix 1 & 2 & 5

6.1.16 Annual reviews should ensure the effectiveness of the CCTV System in relation to its initial purpose, aim and need. Where these aims are no longer met, the CCTV system should be retired, or made fit for purpose.

6.1.17 Any unauthorised access or loss of data, either on the device or on removable media (CD, DVD, USB Pen etc.) must be reported immediately to the Data Protection Lead via ServiceNow as a data breach.

6.1.18 Any complaint received in connection with a CCTV system will be dealt with pursuant to the Customer Feedback Policy unless the issue is directly data protection related in which case it will be handled under the Data Protection Policy by the Data Protection Lead.

6.2 Access to footage and download requests

6.2.1 YHG are occasionally approached by the police and asked for access to CCTV. If there is a trained staff member onsite to support in the viewing of the footage this request should be recorded by YHG staff using the electronic form, Appendix 2. Then assist with viewing of CCTV footage on site with police to support in the detection and investigation of crime. Details recorded within the form include police contact details, staff details, camera location, time and basic details of the incident being investigated.

6.2.2 Trained staff onsite have access to view footage onsite completing the access log via the electronic form or record log held at site. This is to support in any onsite investigations into incidents by managers at site. Appendix 3

6.2.3 Download requests from internal staff using the CCTV Download Request form, Appendix 4, are to be sent to the data protection inbox for processing. Staff will need to provide details of destination of footage and reasoning for the request. The data protection lead will review the request and footage prior to action and release dataprotection@yourhousinggroup.co.uk

6.2.4 External requests are also to be raised via the data protection inbox, requests will be actioned in line with the subject access request procedure. The data protection lead will advise of any delay in this type of request. Where footage is downloaded and released under a formal request YHG will retain a copy of the footage in line with the retention schedule.

7 Responsibilities under this Policy

7.1 The Chief Operating Officer, assisted by the Director of Customer Contact & Experience have overall responsibility to ensure compliance across the Group with this policy and legislation relating to CCTV

7.2 The Director of Asset Management has operational responsibility to ensure the recording of all CCTV Assets & Liabilities across the Group.

7.3 The Data Protection Lead is responsible for the implementation, maintenance and dissemination of this policy.

7.4 Managers and operational staff are responsible for ensuring they and their colleagues comply with this policy in the day-to-day execution of their roles, ensuring the requirements of this policy are explained and complied with by suppliers and contractors. All staff should be aware of this policy, especially any to whom requests for disclosure of CCTV may be made.

7.5 Suppliers and contractors must also comply with current Data Protection legislation where they are implementing, operating or managing CCTV systems on behalf of the Group. The terms of this policy, where appropriate, should be translated into the supplier contracts and requirements, ensuring they're aware of their obligations under the legislation and specifying them as a Data Processor. This must include the ability to evidence their compliance and allow for auditing of their legal compliance.

7.6 Any breach of this policy is a serious matter and may result in disciplinary action being taken by YHG.

8 Risk Management

The risks to YHG in not adhering to this policy is that inappropriate disclosure of CCTV may amount to a serious data breach. In addition, YHG may not effectively reach the full potential of its use of CCTV to assist in protecting its property or in keeping its staff safe.

CCTV is recorded as a risk on the risk register under the GDPR risks.

Risks will be managed by ensuring that staff are familiar with this policy and that CCTV records are managed in accordance with this policy and the Surveillance Camera Code of Practice.

9 Data Protection, Record Storage and Retention

CCTV is specifically covered in the YHG Data retention Policy and associated Schedule.

CCTV stored by the Data Protection Lead after a third-party disclosure request is within the exemptions of the retention policy and will be subject to periodic review by the DP Lead and deleted only when necessary.

10 Equality and Diversity

This policy complies with the requirements of the Equality Act 2010 to ensure equality of treatment for all customers without discrimination or prejudice.

An Equality Impact Assessment has been conducted on this policy.

YHG will provide translations of all its documents, policies and procedures in various languages and other formats on request.

11 Communication

The new Policy will be announced and available to staff via Youggle.

The policy will be announced to tenants via the newsletter and available on the website. It will also be made available in schemes as appropriate.

12 Learning and Development

Training will be given to staff responsible for the management and monitoring of CCTV under this policy.

Relevant line managers for those staff with responsibility as set out above will be responsible for ensuring that this takes place. The Data Protection Lead and other Directors referred to in this Policy will provide support as required with the implementation and rollout of such training.

13 Performance Management of this Policy

There are no key performance indicators associated with this policy.

14 Review of this Policy

This Policy should be reviewed every 2 years by the Data Protection Lead with appropriate consultation with other teams. Reviews may take place sooner if required by changes in legislation, regulation, best practice, case review or as a result of organisational change.

Related Documents

Document Type	Name
Connected Policies and Procedures	**Data protection Policy** **Retention Policy** **Equality, Diversity and Inclusion Policy**
Forms and Letters	**List of attached forms/links** **Appendix 1 – CCTV Viewing and Download Process** **Appendix 2 – Access Log (Police)** **Appendix 3 – Access Log (Staff)** **Appendix 4 – CCTV Download Request** **Appendix 5 – CCTV Review Form**
Leaflets/Publicity Material	**CCTV and Ring Doorbell Flyers now available to support tenants and staff**
Training Materials Available	**CCTV Hub on Youggle** **CCTV Training on Helix**
Intranet/ Website Page	**Data Protection Hub and own page area for CCTV** **DP Working Group - update and roll-out**

Checklist

(To be completed as far as possible by the Policy Author before submission for quality checking by Research and Policy Manager prior to Risk and Compliance Group)

<table>
<tr><td colspan="5">Policy Name: CCTV Policy</td></tr>
<tr><td colspan="2">Version No: 3.0</td><td colspan="3">Effective Date: May 2024</td></tr>
<tr><td colspan="5">Status: Full Review - Ombudsman Order to review download retention when providing police footage</td></tr>
<tr><td colspan="5">Previous Policy Name (where appropriate) n/a</td></tr>
<tr><td colspan="5">Brief Summary of Changes from Previous Version:
Clarification of YHG retaining footage shared with external parties under a formal request</td></tr>
<tr><td colspan="2" rowspan="3">Internal Consultation Groups:

Data Protection Working Group</td><td colspan="3">Customer Consultation: ☐</td></tr>
<tr><td colspan="3">Date of Customer Consultation:</td></tr>
<tr><td colspan="3">Customer Consultation Brief Details:</td></tr>
<tr><td colspan="5">Link to Consultation Document(s):</td></tr>
<tr><td colspan="2">Date Initial Equality Impact Assessment Undertaken:</td><td colspan="3">Equality Impact Assessor name(s):</td></tr>
<tr><td colspan="5">Reason for Decision:</td></tr>
<tr><td colspan="5">Date Full Equality Impact Assessment Undertaken: n/a</td></tr>
<tr><td colspan="5">Brief Outline of any Changes Recommended from EIA:</td></tr>
<tr><td colspan="5">Data Protection/ GDPR Implications: ☒</td></tr>
<tr><td colspan="5">Brief Outline of Data Protection/GDPR Implications:
CCTV policy in place to support the use of CCTV across the group, this policy has been reviewed and reflects the re-wording requested by the Ombudsman. Staff forms and processes have been been reviewed, live links to supporting documents re-freshed and adhere to overall operational use of CCTV.</td></tr>
<tr><td colspan="2">Legal Implications: ☐</td><td colspan="2">Legal Panel Consulted: ☐</td><td>Date:</td></tr>
<tr><td colspan="2">Risk Implications: ☐</td><td colspan="2">Risk Logged on Datix: ☐</td><td>Date:</td></tr>
<tr><td>Resource Implications</td><td>People: ☐</td><td>Finance: ☐</td><td>Asset: ☐</td><td>Other: ☐</td></tr>
<tr><td colspan="5">Brief Summary of how Resource Implications have been addressed:</td></tr>
<tr><td colspan="5">How will communication on this Policy take place: (please delete as appropriate)
Intranet/ YHG Website/ E-Learning/ DP Working Group</td></tr>
<tr><td colspan="3">Policy Owner: Data Protection - Governance</td><td colspan="2">Policy Author: Laura Hughes</td></tr>
<tr><td colspan="4">Policy Quality Checked by Research and Policy Manager:</td><td>Date:</td></tr>
<tr><td colspan="4">Policy Approved by Risk and Compliance Group:</td><td>Date:</td></tr>
</table>

Appendix 1 – CCTV Viewing and Download Process

Appendix 2 – Access Log (Police)

Appendix 3 – Access Log (Staff)

Appendix 4 – CCTV Download Request

Appendix 5 – CCTV Review Form

All available on the CCTV Hub on Youggle