CCTV Policy

Policy name	CCTV Policy
Effective from	May 2026
Effective to	May 2028
Approved by	Risk & Compliance Group
Date approved	19th May 2026
Policy owner/department	Data Protection - Governance
Policy author	Data Protection Lead
Version number	4.0

Version Control

Version	Date	Changes	Reason for the changes	Approver
3.0	May 2024	Review		
4.0	May 2026	New template, DUAA updates and lone working access	Data Use and Access Act 2025 now in place, Lone working access reflected	Risk and Compliance Group

The YHG Plan	
Passionate people ☐	Efficient business ☒
Safe buildings ☒	Viability ☐
Safe environment ☒	Advocating ☐
Secure and connected ☐	Working in Partnership ☒
	Growth ☐

Relevant National Standards or Regulation	• Governance and Financial Viability Standard • Neighbourhood and Community Standard

Relevant Legislation	The policy is to ensure compliance with: • The Data Protection Act 2018, • The Protection of Freedoms Act 2012 • The Home Office Surveillance Camera Code of Practice under the Protection of Freedoms Act • Information Commissioner's Office ("ICO") Code of Practice for Video Surveillance • The General Data Protection Regulations 2018 (UKGDPR) • The Data Use and Access Act 2025 (DUAA)

Partner Responsibilities	Appointed contractors are working under instruction by YHG and are responsible for handling the personal data captured on CCTV systems in a safe and secure manner. Access to footage, including collection of footage under instruction, must be recorded with a clear access audit trail. Where systems are in premises supporting external customers, system access will be reviewed by the Data Protection Lead (DPL) and partners who are granted access to view and investigate issues at site would be required to complete the CCTV training, therefore holding the same responsibilities as a YHG employee.

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

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

2.2 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.

2.6 The Group does not use General Covert CCTV.

YHG support Anti-Social Behaviour and criminal investigations where necessary. In cases where Directed Covert CCTV is required by an external investigating agency (Police), YHG will review each request on a case-by-case basis, taking into consideration the privacy and safety of customers. The owners of the systems will have overall responsibility for the footage captured in this type of case.

2.7 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, body worn video, biometric characteristic recognition or facial recognition etc. Where use of this type of technology is being considered, colleagues 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.

2.8 This policy will cover: -

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

2.9 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 Tenancy Management Officer for consideration who may also direct the tenant to the Information Commissioners Office for further guidance on use of CCTV. A Customer CCTV/Ring Doorbell flyer and a responsibilities leaflet is available for customers operating domestic CCTV.

3 Definitions

Overt CCTV: Overt surveillance is carried out with the full knowledge of colleagues, 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. Dashcams are fitted in YHG owned or leased vehicles and fall under the same process as building mounted cameras. On-going observation of the CCTV images may be required, for example at night during lone working hours, 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 previously been approved by the Risk and Compliance Group. Reviewed by the Data Protection Working Group, ASB team and Housing Management team during March 2026.

5 Background and Context

This policy has been reviewed as part of the planned review procedure. 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 Home Office Surveillance Camera Code of Practice under the protection of Freedoms Act 2022, 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 colleagues 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 YHG's 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 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 is permitted at site where the YHG employee has completed the CCTV training and is accessing the footage for a legitimate reason, documenting this for a clear audit trail of system access.

c. Where there are lone workers at a site or scheme overnight, a restricted view of CCTV will be made available to support the safety and security of customers, employees and contractors. The view of the footage must be kept secure with a restricted view.

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. The Data Protection team hold the retained footage on central systems with restricted access.

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 colleagues have access to CCTV systems, and all colleagues should ensure the legitimacy of external support and maintenance colleagues who are granted access to the CCTV system(s).

6.1.12 Appropriate inductions and training will be provided to all authorised Group colleagues who deal with the CCTV systems. This includes communication of

relevant policies and procedures. Training is available on Helix for all employees and mandatory for specific roles across the group.

6.1.13 CCTV systems should be regularly maintained:

a. The appointed contractor or employee at site or scheme 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. They will use the electronic form available on the CCTV Hub.

6.1.15 A record should be maintained of all actions carried out against the CCTV system, whether maintenance, support tasks or data retrieval. Available on the CCTV Hub: CCTV Process Charts, Access Logs, Download form and Review Form

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 (USB Pen etc.) must be reported immediately to the Data Protection Lead via service now 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 Out of Hours CCTV requests

6.2.1 YHG are, occasionally, approached by the police and asked for access to CCTV. If there is a trained colleague onsite to support in the viewing of the footage this request should be recorded, and footage viewed to support in the detection and investigation of crime.

6.2.2 On the CCTV Hub is a link to an electronic form that can be completed by internal colleagues to log 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, colleague details, camera location, time and basic details of the incident being investigated. Once completed the form will send an alert to the DP Lead notifying of the access to the system at site.

6.2.3 Trained colleagues onsite have access to view footage onsite completing the access log via an electronic form or a paper-based form at site. This is to support in any onsite investigations into incidents by managers at site.

6.2.4 Download requests using the CCTV Request form are to be sent to the data protection inbox for processing dataprotection@yourhousinggroup.co.uk

7 Responsibilities under this Policy

7.1 The Chief Executive Officer, assisted by the Executive Director of Housing & Customer 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 colleagues 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 colleagues 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 colleagues safe.
CCTV is recorded as a risk on the risk register under the GDPR risks.

Risks will be managed by ensuring that colleagues are familiar with this policy and that CCTV records are managed in accordance with this policy and the Home Office Surveillance Camera Code of Practice under the Protection of Freedoms Act

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 team 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 (normally six months after external release).

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. The YHG website also has an accessibility option for translations to support access and understanding for all.

11 Communication

The new Policy will be announced and available to colleagues 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 colleagues responsible for the management and monitoring of CCTV under this policy.

Relevant line managers for colleagues 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 YHG Drivers Handbook - Dashcams
Forms and Letters	CCTV Flow/Process Access Log (Police) Access Log (Colleagues) CCTV Download Request CCTV Review Form Dashcam download Process All available on the CCTV Hub
Leaflets/Publicity Material	
Training Materials Available	CCTV training available on Helix
Intranet/ Website Page	Data Protection Hub and CCTV Hub on Youggle