Red Kite Community Housing

URN: POL019

CCTV Policy - Overt Systems

Partnership • Respect • Pride

Realising the potential in our communities

1. Purpose

1.1 This policy is one of three that cover our use of Closed Circuit Television (CCTV). The other two are

- CCTV – covert systems
- CCTV – Small Unmanned Aerial Systems (SUAS) - *Drone*

1.2 This policy outlines how we meet legislative requirements in the installation of CCTV.

1.3 This policy outlines how we deploy and manage our overt CCTV systems.

1.4 This policy outlines what criteria will be used for the deployment of overt CCTV. This balances:

- Our ambition to protect community safety
- The impact our systems will have on the privacy of individuals
- Value for Money

1.5 This policy outlines how we will meet Data Protection requirements through:

- Clear ownership
- Clear purpose
- How privacy will be maintained
- Clear management guidelines
- Maintenance and calibration
- How images are used
- How individuals access CCTV images

2. References

2.1 Information Commissioners Office, the Circuit Television (CCTV) – Management and Operation – Code of practice 2015.

2.2 Home Office Surveillance Camera Code of Practice Responsibilities

Role	Responsibility
System Owner	• Experience Manager
Carrying out Privacy Impact Assessments	• Experience Manager • Senior ASB Specialist • Member of Environment Improvement Group (where possible)
Authorising the reviewing of images	• Data Protection Officer
Replying to Subject Access Requests	• Data Protection Officer
Authority to disclose data	• Data Protection Officer & Experience Manager
Completion of Business Case	• Senior ASB Specialist
Viewing of images	• Experience Manager • Senior ASB Specialist • ASB Specialist • Data Protection Officer
Viewing of images for maintenance / testing purposes	• IT Manager

2.3 All relevant staff will have appropriate training to carry out their role in relation to CCTV.

3. Legal and Regulatory Framework

- Data Protection Act 1998
- Human Rights Act 1988
- Regulator of Social Housing Regulatory Standards
- Protection of Freedoms Act 2012
- UK Government: Home Office Surveillance Camera Code of Practice (2013)
- Information Commissioner Office – CCTV Code of Guidance
- General Data Protection Regulation (2018)

- As a Housing Association Red Kite not subject to Regulation of Investigatory Powers Act 2000

4. Definitions

- ASB – Anti-social behaviour
- CCTV – Closed Circuit Television
- Overt surveillance – surveillance that is openly carried out with clear signage
- Covert surveillance – surveillance that is carried out without clear identification or signage
- Privacy Impact Assessment – an assessment used to determine the impact on privacy through the installation/use of CCTV in an area. This will be used to decide if the use of CCTV is warranted
- ICO – Information Commissioners Officer
- Data subject – a person who has been recorded on CCTV and whose information is stored (i.e. images)
- SUAS – Small Unmanned Aerial Surveillance (also known as a 'drone')
- Data controller – the company / organisation who has responsibility for data or information stored and used of individuals
- Date processor – the company / organisation that is processing the data of the data controller (this can be the same as the data controller)
- Passive monitoring – when CCTV footage is reviewed after event for specific purposes (i.e. not viewed in real time or live)

5. Key Principles

5.1 We use CCTV surveillance systems to deter and detect crime and anti-social behaviour, and to improve community safety.

5.2 We comply with ICO Code of Guidance

5.3 We have notified the ICO we are a Data Controller and renew this notification annually.

5.4 We are both Data Controller, in that we make decisions on how the system is used and the information managed, and the Data Processor, in that we operate the system and manage the information collected through our CCTV systems.

6. Policy Statement

6.1 Our CCTV system

6.2 We hold a CCTV register that covers each site with CCTV in operation. This covers

- CCTV Business Case
- Privacy Impact Assessment
- Site Checklist
- ICO Notification
- CCTV equipment in place
- Record of CCTV system quality checks

6.3 No camera will be hidden from view and all will be prevented from focussing on private areas.

6.4 Signs will be prominently placed at strategic points and at entrance and exit points of the sites to advise residents, visitors and members of the public that a CCTV system is in use. This will display

- We are the owner
- The purpose of the CCTV
- Our website and phone number

6.5 Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

6.6 The system will be passively monitored.

6.7 Live images / footage will viewed for the following purposes only

- Training
- Servicing / maintenance purposes
- A request from the Police (if part of an investigation or to aid the prevention/ detection of a crime),
- Daily site check where CCTV is installed to deter fly tipping

7. Purpose of the system

7.1 We will install systems with the primary purpose of reducing the threat of crime generally, protecting our property and homes, and to improve public safety.

7.2 These purposes will be achieved by monitoring the system to:

- Deter crime
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and community safety.

7.3 The system will not be used:

- For any purpose other than laid out above
- To provide recorded images for the Internet.
- To record sound
- For any automated decision taking

8. Installation of systems

8.1 New systems will be introduced if

- There is a specific need that cannot be met through other reasonable methods
- A Privacy Impact Assessment is carried out
- There is a robust business case

9. Storage of images

9.1 Images will be stored either

- on site using secure digital recorders
- off-site with data transmitted via the Internet on secure servers

9.2 Images will be time/date stamped

9.3 Images will be stored for a maximum 28 days (it will be stored longer following a request from the Police or if we are replying to a Subject Access Request)

9.4 Images will be automatically deleted after this period

10. Access to images

10.1 Only nominated persons (see section 3 – Responsibilities) will have access to images (either live or stored)

10.2 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded may assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime in consultation with the Police or Community Safety Partnership.
- Emergency services in connection with the investigation of an accident.

11. Access to images by a subject

11.1 CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Act. We will provide images in line with our Subject Access Request process.

11.2 Images can only be provided if it will not be prejudicial to criminal enquiries or proceedings. We will obscure third parties where appropriate.

11.3 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. They need to give the following information to enable us to find their image:

- Location
- Time
- Date
- Photograph of the subject so we can identify them in the footage

11.4 The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant within forty days of receiving the required fee and information.

11.5 The Data Protection Act gives the Data Protection Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

11.6 All such requests will be referred to the System Owner by the Data Protection Officer.

11.7 If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

11.8 At times we may provide data to individuals for their use in civil or insurance claims, but only if it is justifiable and does not put others' safety at risk. We do not obscure images within our system, so if others can be identified we will not provide this data.

11.9 We hold a Data Request Register that outlines:

- Date of request
- Who requested the data?
- Why they requested the data
- Our response

Staff roles listed in the **Competency Standards section** must be acquainted with contents of this document and have had documented instructions and training on its use. Authority to amend can only be undertaken by the **Process owner** with the relevant **Delegated approvals**.

For information on interpretations and instructions staff should contact the **Subject Matter expert** or **Process owner** and under no circumstances should any deviation be permitted without prior approval as above.

Document Controls			
Version:	2	**Effective date:**	February 2021
Subject Matter expert drafter:	**Data Protection Officer**	**Process owner :**	**Governance and Regulation Manager**
Related Pod	Community	**Related Policy**	Data Protection Policy IT Policies Anti-Social Behaviour Policy Subject Access Request process Customer Guidance on CCTV CCTV – Covert Systems CCTV Small Unmanned Aerial Systems (SUAS) - *Drone*
Review period	12 months	**Next review due by:**	December 2023
Delegated approvals			
The 3 lines of defence have been checked within the framework and are valid			☐
Approved by AD	N/A	**Approved Date:**	N/A
Approved by EMT	Ray Prior 	**Approved Date:**	12/03/2021
Approved by Board/ Committee/RRT	N/A	**Approved Date:**	N/A

Competenacy Standards			
Roles using this document	• Experience Manager • Senior ASB Specialist • ASB Specialist • Data Protection Officer • IT Manager	**Mandatory training frequency**	12 months
Associated legislation	• Data Protection Act 1998 • Human Rights Act 1988 • Protection of Freedoms Act 2012 • UK Government: Home Office Surveillance Camera Code of Practice (2013) • Information Commissioner Office – CCTV Code of Guidance • General Data Protection Regulation (2018)	**Vocational training frequency**	e.g. 1 x specialist training course annually
Consumer Standards	Neighbourhood Standard	**Other**	

Lines of Defence	
Lines of Defence	**Evidence**
Lines of defence 1	1. Policy approved, with relevant cover sheet. 2. All relevant staff briefed and trained on the policy, forming part of inductions for new staff. 3. Assessment during 121 sessions. *4.* Reporting process for breaches of the policy.
Lines of defence 2	5. GROW team to provide exception report on training on monthly basis to Heads of Service and Policy Owner 6. Any breach of the policy reported to Company Secretary.
Lines of defence 3	*7.* Audit programme – audits will identify any housekeeping or recommended actions relating to non-compliance with all policies.