CCTV POLICY

Red Kite Group Use of CCTV

Partnership • Respect • Pride
Realising the potential in our communities

1. Definitions

ASB	Anti-social behaviour
CCTV	Closed Circuit Television. We include video doorbells within this definition.
Surveillance	Surveillance that is openly carried out with clear signage
PIA / 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 Commissioner's Officer
Data subject	a person who has been recorded on CCTV and whose information is stored (i.e. images)
Data controller	the company / organisation who has responsibility for data or information stored and used of individuals
Data 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)
DPA 2018	Data Protection Act 2018
GDPR	General Data Protection Regulation

2. Purpose

This policy outlines:

2.1. How we meet legislative requirements in the installation of CCTV.

2.2. How we deploy and manage our CCTV systems.

2.3. What criteria will be used for the deployment of CCTV, balancing:

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

2.4. 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
- How we will manage CCTV at our tenant's homes in line with data protection requirements.

2.5. This policy applies to all CCTV used in offices, on developments, on schemes, and by tenants. It covers all stages of using CCTV.

3. Policy Statement

3.1. Red Kite Community Housing (Red Kite) will comply with all relevant data protection legislation and guidance at all stages of using CCTV, including:

3.2. When we decide to implement a new CCTV system; how we use the system; how we tell people about it; and how we share the images.

3.3. Our tenants may also choose to use their own CCTV systems, and we will offer advice on how to do so appropriately.

4. Our CCTV system

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

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

4.3. Signs will be prominently placed at strategic points and at entrance and exit points of the sites to advise tenants, 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

4.4. 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. We will monitor and review footage for the purposes set out below.

5. Purpose of the system

5.1. 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.

5.2. These purposes will be achieved by monitoring the system to:

- Prevention of crime
- Training
- Service / maintenance purposes
- Detection of crime – e.g. a request from the police
- Reduce the threat of ASB
- Deter fly-tipping
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and community safety.

5.3. 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

6. Installation of systems

6.1. 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

7. Storage of images

7.1. Images will be stored either

- on site using secure digital recorders
- off-site with data transmitted via the Internet on secure servers
- Images will be time/date stamped
- Images will be automatically deleted when they are no longer required, in line with GDPR

8. Equality & Diversity Statement

8.1. We are committed to treating people fairly, without bias or discrimination, and always within the law. We promote equality of opportunity for all our customers and stakeholders, regardless of their race, gender, age, religious belief or non-religious belief, ethnic origin, disability, marital status, or sexual orientation. In addition to any statutory responsibilities under the Equality Act 2010 (and any other relevant legislation), we will also act in accordance with our own provisions in relation to equality and diversity.

9. References

- Privacy & Data Protection Policy
- Privacy Notice

10. Responsibilities

All staff are responsible for complying with this policy.

11. Legal and Regulatory Framework

- Data Protection Act 2018
- Human Rights Act 1998
- 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 are not subject to the Regulation of Investigatory Powers Act 2000

12. Red Kite use of CCTV

12.1. We use CCTV surveillance systems to deter and detect crime and anti-social behaviour, and to improve community safety. However, we do not assume that CCTV will always be the most appropriate option to address an existing or possible issue. For example, security may be improved by fencing and lighting solutions. A Privacy Impact Assessment (PIA) will be carried out to establish if CCTV is appropriate in the circumstances.

12.2. When it is appropriate to use CCTV to address a particular issue, we will review the need for the CCTV at regular intervals, or when the situation significantly changes. For example, if anti-social behaviour reduces due to a perpetrator leaving the area, it may be possible to remove the CCTV.

12.3. Red Kite does not have the legal powers required to use covert CCTV.

12.4. There may be some circumstances when the Police or other law enforcement agency ask for our co-operation with a covert surveillance exercise, which we will consider on a case-by-case basis.

12.5. Systems should be able to record good quality images, of the appropriate standard to be used for the reasons the CCTV is in place.

12.6. Cameras should be positioned to allow areas of interest to be filmed unobscured, but to ensure that areas that are not of interest or should not be filmed, such as private homes, are not filmed. If the cameras cannot be sited in a way that avoids filming private areas, technical solutions should be used to obscure the private areas.

12.7. Monitors that display images should be positioned so they can only be viewed by authorised staff, unless they show an area that can be seen from where the monitor is positioned. For example, if a monitor only shows an office reception area, the monitor can be visible to anyone in that reception area. If the monitor also shows a corridor that is through a door from the reception area and therefore can't be seen from the reception, the monitor should be positioned so it cannot be viewed by anyone except authorised staff.

12.8. Recorded footage should be stored securely, so it can only be accessed by authorised staff.

12.9. Using CCTV is a form of processing personal data, or information about people. 'Processing' includes anything that can be done to personal data, from collecting, through storing, using and sharing, to disposing of personal data.

12.10. Each stage of data processing must be carried out in compliance with data protection legislation, including the GDPR and the DPA 2018.

12.11. We will only process data if there is a lawful basis to do so, and we will tell people about how their data is being processed via our Privacy Notice and CCTV signage.

12.12. The GDPR Principles:

- Purpose limitation – only using data for specific purposes;
- Data minimisation – only collecting and using minimum data;
- Accurate and up to date data;
- Storage limitation – only retaining data as long as necessary;
- Security – keeping data secure, in storage and when being accessed or shared;
- Accountability – meaning being able to demonstrate compliance with the other requirements of the legislation.

12.13. The GDPR Rights of Individuals that are applicable to CCTV include:

- The Right to Access – giving people access to their own data, which is the footage that they appear in;
- The Right to Erasure – allowing people to ask for it to be erased.
  Note: Some exemptions do apply when responding to these requests.

12.14. The GDPR requires specific controls to be in place whenever 'Data Processors' are used. A third party who operates CCTV on behalf of Red Kite is a Data Processor, and Red Kite is responsible for: selecting companies who provide sufficient guarantees that they will comply with data protection legislation; including GDPR compliant clauses in the contract; continuing to manage and review the contract.

13. Sharing CCTV footage with external agencies:

13.1. All requests for access to CCTV footage will be considered in line with the GDPR Principles as above. It is key to identify a lawful basis for the sharing, to meet the first principle of 'lawful, fair and transparent processing'. Identifying the lawful basis may mean referring to the DPA 2018 as well as the GDPR, as the DPA 2018 contains a number of clarifications and exemptions to the GDPR.

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

13.3. 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.

13.4. 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.

14. Access to images by a subject

14.1. 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.

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

14.3. A person whose image has been recorded and retained and who wishes to have 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

14.4. 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, where applicable, and information.

14.5. 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.

14.6. All such requests will be referred to the Data Protection Officer.

14.7. 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.

14.8. 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. If others can be identified we will not provide this data.

14.9. We hold a Data Request Register that outlines:

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

15. Tenant use of CCTV

15.1. More information about how we oversee CCTV installed by our tenants at their homes can be found in our CCTV Tenant Use Policy.

16. CCTV footage shared with us

16.1. We will only keep copies of footage that is relevant, and that we need as evidence; anything irrelevant or excessive will be deleted and we will inform the person who sent it to us that it has been deleted, explaining why.

16.2. If we receive footage from domestic CCTV, video doorbells or mobile phone cameras, or similar, we become the Data Controller of the data contained in the footage and must comply with all data protection legal requirements, including complying with the (UK) GDPR Principles, upholding data subjects' rights, and controlling data transfers appropriately.

16.3. The (UK) GDPR rights of individuals that apply to CCTV.

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:	3	**Effective date:**	May 2024
Subject Matter expert drafter:	Head of Governance	**Process owner:**	Head of Governance
Related Pod	Community	**Related Policy**	Privacy & Data Protection Policy IT Policies Anti-Social Behaviour Policy Subject Access Request process Customer Guidance on CCTV
Review period	3 years	**Next review due by:**	May 2027
Delegated approvals			
The 3 lines of defence have been checked within the framework and are valid ☐			
Approved by EMT	**Blaise Jennings**	**Approved Date:**	**22nd May 2024**
Approved by Board/ Committee/ RRT		**Approved Date:**	