Surveillance Camera Systems Policy

1.0 Purpose of policy

1.1 As the general Surveillance Camera Systems Policy of the Karbon Homes Group "The Group", this document sets out the accepted use and management of Surveillance Camera Systems and its associated images and sound to ensure that whilst complying with the General Data Protection Regulation and other associated Data Protection legislation it also acts in accordance with the Human Rights Act (1998) to provide a safe and secure environment for staff and visitors to the Group's premises.

1.2 The Policy also outlines how Surveillance Camera Systems will be used to protect the Groups property and to investigate breaches of tenancy or employment conditions and anti-social behaviour.

2.0 Objectives

2.1 We currently use Surveillance Camera Systems as outlined in this policy. We believe that such use is necessary for legitimate business purposes, including;

- to help deter and / or detect crime, anti-social behaviour or breaches of contract;
- to provide evidential material for court or alleged misconduct and / or holding disciplinary hearings;
- to help reduce the fear of crime;
- to provide assistance in the overall management of public safety; and
- to enhance community safety.

This list is not exhaustive and other purposes may be or become relevant.

3.0 Policy detail

The Group will lawfully collect and process images and sounds captured on the Surveillance Camera Systems that it operates in compliance with the legally enforceable data protection principles of the GDPR.

The Group will provide help to staff and members of the public to exercise their rights under the GDPR.

The Group will consider the HRA, specifically the right to respect for private and family life, when considering where to operate its Surveillance Camera Systems.

The Company Secretary is responsible for implementing this policy. Karbon Homes' Compliance Specialist (Asset & Regeneration) has responsibility for complying with the ICO's CCTV Code of Practice.

The Group will train staff appointed to process and interpret surveillance camera images for the purposes identified above.

3.1 Position of fixed Surveillance Camera Systems

The Group will only position fixed CCTV cameras to cover the Group's property and land.

The Group will clearly display signs for CCTV cameras so staff and visitors are aware they are entering an area covered by fixed Surveillance Camera Systems.

The Group will provide the necessary contact information for the public to make enquiries about the use of cameras.

The Group will position the cameras so they are secure and protected from vandalism and kept in working order.

Only in exceptional circumstances and in order to deal with very serious concerns will the Group use surveillance cameras in areas where people have a high expectation of privacy including office environments; this will only be done with the express permission of a suitably qualified person.

3.2 Images

The equipment will record standard surveillance camera images which, under optimum conditions, are effective for the purpose for which they were intended.

Each system will receive a planned preventative maintenance inspection by a competent person to carry out an audit and ensure the system is in full working order. A report will be created for each site visit which will list any defects and comments regarding the functionality of the system.

The frequency of visits will depend on the complexity of the system and the environmental conditions the equipment may be subjected to.

All images are either digitally recorded and stored securely within the Surveillance Camera Systems hard drives for 31 days or recorded on a loop system which records for up to 60 days before they are automatically erased. A suitably qualified person may authorise a copy to be taken and stored securely when the images have been requested for legal or alleged misconduct and / or holding disciplinary hearings. Images and recording logs will be held in accordance with the Group's Data Protection policy and Data Retention schedule.

All digital recordings will be date and time stamped.

3.3 Covert recording

The Group will only undertake covert recording with the written authorisation of a suitably qualified person where:

- telling someone that we are making the recording would seriously prejudice the reason for making the recording; or
- there is good cause to suspect that an illegal or unauthorised action(s) or breach of contract, anti-social behaviour or crime and disorder is / are taking place or about to take place.

We will comply with the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) when operating covert Surveillance Camera Systems.

We will only carry out such recording for a limited and reasonable amount of time consistent with the objectives of the monitoring and only to detect a specific activity.

We will fully document all covert recordings showing who made the decision to use covert monitoring and why.

3.4 Access to and disclosure of images/sounds to third parties

We will restrict and control access to and disclosure of images and sounds recorded on Surveillance Camera Systems. This will ensure the rights of individuals are retained and safeguard the security of the images so they can be used as evidence if needed.

We will only disclose images/sounds according to the purposes for which we originally collected them.

3.5 Access to images/sounds

We will restrict who can see/hear recorded images/sounds to those staff approved to view/listen to them.

Viewing/listening of recorded images/sounds will take place in an area to which other employees will not have access while viewing/listening is occurring.

We will document when any medium on which images/sounds are recorded is removed for viewing/listening purposes.

We will protect images/sounds removed as evidence in secure storage.

As part of door entry systems there may be fixed surveillance cameras installed which do not record images or sounds and instead relay this information to resident's accommodation for live viewing.

3.6 Disclosure of images/sounds

Only suitably qualified persons can authorise disclosure of images or sounds to third parties or members of staff.

Disclosures to third parties or members of staff will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

- Police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.
- Prosecution agencies.
- Relevant legal representatives.
- People whose images/sounds have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings).
- In exceptional cases, to others in order to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident or incident of anti-social behaviour or disorder.
- Members of staff investigating or involved in alleged misconduct and / or disciplinary hearings.

All requests for disclosure will be documented. If disclosure is denied, the reason will also be recorded.

3.7 Individuals' access rights

The DPBP is responsible for managing data subject access requests and other data subject rights under Data Protection legislation relating to surveillance video images and sounds.

The Group will aid staff and members of the public to seek access to surveillance video images and sounds of themselves and respond within the legal time limit of a calendar month once we have received a request.

The Group will consider a data subject access request once it has been received in writing (written with help from our staff or a third party if required) and is accompanied by:

- suitable evidence to identify the person making the request; and
- a photo or description of the person so we can find their image on the surveillance cameras recording.

We reserve the right to obscure images of third parties when disclosing surveillance camera data as part of a subject access request, where we consider it necessary to do so.

3.8 Requests to prevent processing

We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of GDPR). For further information regarding this, please contact the DPBP.

4.0 Monitoring and Review

All staff members must observe this policy and the DPBP has overall responsibility for this policy. The DPBP will monitor it regularly in collaboration with the Company Secretary and Compliance Specialist (Asset & Regeneration) to make sure it is being adhered to and the policy will be reviewed in accordance with changes in legislation or best practice.

Performance will be reported to the Group Audit and Risk Committee on an annual basis.

5.0 Equality and Diversity

This policy is implemented in line with the Group's Equality and Diversity Policy and associated legislation. Consideration will be given to all protected characteristics under the Equality Act 2010 to eliminate discrimination, advance equality of opportunity and foster good relations.

This policy and associated documents are available in different languages and alternative formats where necessary.

6.0 Data Protection and Privacy

We have a clear policy on data protection and sharing data with other partners/outside agencies under the requirements of the General Data Protection Regulation. This is clearly set out in our Data Protection policy which, along with the supporting Data Protection procedures, must be followed throughout the operation of this policy.