# POLICY: CCTV AND DRONES (UAD's) USE

## Sections



Copies of this Policy may be made available in alternative formats on request.


| | |
|---|---|
| Previously agreed by The Board: | 27 July 2022 |
| Previously approved by the Board: | 21 September 2022 |
| Agreed by the Board | 27 January 2025 |
| Approved by the Board | 21 May 2025 |
| Next review date: | January 2028 |
| Published on website: | Yes |

# POLICY: CCTV AND DRONES (UAD's) USE

All reference to 'we', 'our' or 'us' in this Policy should be read as meaning Sandbourne Housing Association.

The term 'premises' includes offices, and all sites and schemes owned or controlled by Sandbourne.

For the purposes of this Policy reference to 'CCTV' includes video surveillance systems that may also be used on occasion.

## 1. Purpose and aim of the Policy

1.1 We use closed circuit television (CCTV) images to help provide a safe and secure environment for employees, residents and for visitors to our premises, such as clients, customers, contractors and suppliers, and to protect our property. We may also use CCTV to monitor particular areas such as lifts for safety reasons.

Currently we do not use drones or unmanned ariel devices (UAD's) but may do so in the future, to help us undertake property surveys or diagnose building defects at height.

1.2 This policy sets out the use and management of the CCTV equipment, drones and the images they take in compliance with the Data Protection Act 2018, GDPR requirements and the CCTV Code of Practice.

1.3 Our CCTV facility record images only. There is no audio recording i.e. conversations are not recorded on CCTV (but see the section on covert recording).

## 2. Purposes of CCTV and drones

2.1 The purposes of our installing and using CCTV systems include:

2.1.1 To assist in the prevention or detection of crime or equivalent anti-social behaviour and provide evidence of the same.

2.1.2 To assist in the identification of offenders that may lead to prosecution or enforcement action in accordance with the tenancy agreement.

2.1.3 To monitor the safety, security and operation of our equipment and use of our premises.

2.1.4 To help ensure that health and safety and our procedures are being complied with.

2.1.5 To assist us in the identification of unauthorised actions or unsafe working practices by anyone that might result in disciplinary, or training proceedings being instituted against employees, contractors, or others and to assist in providing relevant evidence in cases of suspected criminal or similar activity such as anti-social behaviour by tenants or visitors.

2.1.6 Drones may be used to assist us in the future survey of the external areas of our homes.

## 3. Location of CCTV cameras

3.1 Cameras are located at strategic points throughout our premises, principally at the main entrance and exit points. We have positioned the cameras so that they only cover communal or public areas on our premises, and they have been sited so that they provide clear images. No camera focuses, or will focus, on toilets, shower facilities, changing rooms, staff kitchen areas, staff break rooms or private offices.

3.2 All cameras (except for any that may be temporarily set up for covert recording as described at section 7) are also clearly visible.

3.3 Appropriate signs are prominently displayed so that employees, clients, customers and other visitors are aware they are entering an area covered by CCTV.

## 4. Recording and retention of images

4.1 Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above.

4.2 Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images.

4.3 Images may be recorded either in constant real-time (24-hours a day throughout the year), or only at certain times, as the needs of the business dictate.

4.4 As the recording system records digital images, any CCTV images that are held on the hard drive of a PC or server are deleted and overwritten on a recycling basis and, in any event, are not normally held for more than one month. Once a hard drive has reached the end of its use, it will be erased prior to disposal.

4.5 Images that are stored on, or transferred on to, removable media are erased or destroyed once the purpose of the recording is no longer

relevant. In normal circumstances, this will be a period of one month. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

## 5. Access to and disclosure of images

5.1 Access to, and disclosure of, images recorded on CCTV or by a drone is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected or at the request of a statutory law enforcement agency.

5.2 The images that are filmed are recorded centrally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system or drone and to those line managers who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

5.3 Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

5.3.1 Lawful disclosure, for example, the police and other law enforcement agencies, where for example the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.

5.3.2 Prosecution agencies, such as the Crown Prosecution Service.

5.3.3 Relevant legal representatives.

5.3.4 Line managers involved with our disciplinary and performance management processes.

5.3.5 Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

5.4 The Chief Executive (CEO), or other senior designated officer(s) are the only persons permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

5.5 All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

## 6. Individuals' access rights

6.1 Under the Data Protection Act 2018 (GDPR), individuals have the right on request to receive a copy of the personal data that we hold about them, including CCTV or drone images if they are recognisable from the image.

6.2 Anyone wishing to access any CCTV or drone images relating to themselves, must make a request to our Data Protection Officer (CEO). The request must include the date and approximate time when the images were recorded and the location of the CCTV camera, so that the images can be easily located, and the individual's identity can be established as the person in the images. We will respond promptly to such requests and, in any case, normally within 28 days of receiving the request.

6.3 We will always check the identity of the person making the request before processing it.

6.4 The Data Protection Officer (CEO) will first determine whether disclosure of images will reveal third party information as normally an individual has no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

6.5 If we are unable to comply with the request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, the individual making the request will be advised accordingly.

## 7. Covert recording

7.1 We will only undertake covert recording with the written authorisation of the Chief Executive or other designated senior officer(s) where there is good cause to suspect that criminal activity or equivalent anti-social behaviour or malpractice is taking, or is about to take, place and informing anyone including the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection.

7.2 Covert monitoring may include both video and audio recording.

7.3 Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of particular suspected criminal activity or equivalent anti-social behaviour or malpractice. Once the specific investigation has been completed, covert monitoring will cease.

7.4 Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent anti-social behaviour or malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which we cannot reasonably be expected to ignore.

## 8. Use of drones

8.1 Drones will generally only be used in connection with establishing property condition or building defects. However, in doing so it is possible images / footage of identifiable individuals may also be recorded, constituting personal data in accordance with the Data Protection Act 2018.Therfore, as with CCTV images the Data Controller is responsible for ensuring that there is legal justification for the use of a drone and that we only process the information that we need.

8.2 Any contractor or third party that we use for this purpose will be required to evidence that they are registered with the Civil Aviation Authority and provide us with their Flyer ID. They will also be required to provide a copy of their Public Liability Insurance which must meet our requirements.

8.3 We will carry out a data protection impact assessment (DPIA) to be satisfied that the use of a drone is justified. The Data Controller will need to be satisfied that use of a drone is proportionate to the circumstances, and there is a legal basis for doing so.

8.4 Where a drone is be used, we will give residents advanced notice of this by means of a letter, email or notice in a communal area, and refer them to our Privacy Notice on our website.

8.5 Wherever possible we will use a drone that has an “on/off” facility, to help ensure that only the footage that is absolutely necessary is recorded.

8.6 We will take the practical steps we can to ensure that any captured data is secure in the event of the drone crashing and being taken by an unauthorised third party.

## 8. Training

8.1 We will ensure that all employees handling CCTV images or recordings are trained in the operation and administration of the CCTV system and on the impact of the Data Protection Act 2018 (GDPR) with regard to that system.

## 9. Implementation

9.1 Our Chief Executive is responsible for the implementation of, and compliance with, this policy and the operation of the CCTV system and will conduct a regular review of our use of CCTV. Any complaints or enquiries about the operation of our CCTV system or drones should be addressed to us.

## 10. Equality impact assessment/Protected characteristics (as at 8 January 2025 or later amendments/additions)

10.1 Neutral.

## 11. Consultation arrangements

12.1 We will consult residents on significant changes to this policy and their views will be taken into account by the Board before adopting it. Our employees will also be consulted on significant changes to this policy and any reasonable suggestions will be taken into account before the policy is approved by the Board.