Policy No: SJD/ORG/05	Authorised by: Davina Powell	Review Date: 1st August 2023
Policy Date: 12 April 2021		Date of Next Review: 1st August 2024
CCTV		

Purpose

The purpose of this policy is to regulate the management and use of the closed-circuit television (CCTV) system at SJD Homes on all sites.

The SJD Homes policy is that there will be no electronic surveillance equipment in the home that will be used to monitor the movements or identify the location of young people. The only exceptions to the above are:

Where a child / young person is subject to electronic monitoring imposed by a Court; and

Where it can be explicitly demonstrated with the consent of the child's placing authority, in writing, that such equipment is absolutely necessary to protecting and safeguarding the child's welfare.

Any monitoring or surveillance will be no more intrusive than necessary, having regard to the child's need for privacy.

The CCTV system comprises a main control unit and fixed cameras located strategically internally and external to the house. It is a digital system which is owned wholly by the Company and is entirely closed with no wireless capability. The system does not make audio recordings. All cameras are situated in communal areas only, there are no cameras in private living areas or staff sleep-in rooms.

Statement

It is our policy to have closed circuit television (CCTV) installed at all of our sites for use when required. The cameras that are used by the Company are of an overt nature, the purpose of using CCTV is to ensure that our service users, team members, visitors and professionals are afforded the best possible security and safety whilst visiting or living within our premises. CCTV on our sites is never used as a substitute for trained and well supported staff members. Instead, it is used as an extra layer of security for those people as stated above.

This policy and procedure should be read in conjunction with information provided by the IC0 (Information Commissioner):

- *'A data protection code of practice for surveillance cameras and personal information',*
- *'Conducting Privacy Impact Assessments'*
- *CQC 'Using Surveillance'*

We have considered the *Data Protection Act 1998 ,* the *Human Rights Act 1998,* and the *Health & Social Care Act 2008* when writing the policy and procedure.

1. Registration with the IC0

We are registered with the Information Commissioner under the terms of the *Data Protection Act 1998* and are committed to complying with the requirements both of the *Data Protection Act* and the *Commissioner's Code of Practice*, as well as the *Surveillance Camera Code of Practice 2015* published by the Home Office.

2. CCTV Recordings as 'Data'

Materials or knowledge secured as a result of CCTV will not be released to the media, nor used for any commercial purpose, nor for the purpose of entertainment. Recordings will only be released under the written authority from the Police, or in respect of a subject access request.

Signage, as required by the *Code of Practice of the Information Commissioner* have been placed at all access routes to areas covered by our CCTV.

3. Operation of the System

The systems will be administered by the Registered Manager in accordance with the principles and objectives expressed in the code.

The Manager will check on a regular basis that the system is operating effectively and in particular that the equipment is properly recording and that cameras are functional. The system will be regularly serviced and maintained.

4. **Control of Software and Access to the System**

Access to the CCTV software will be strictly limited to authorised operators, usually the Service Manager, who must satisfy themselves that all persons viewing CCTV material will have a right to do so. The main communication cupboard that houses the CCTV facility must be kept locked secure when not in use. Other administrative functions will include controlling and maintaining downloaded digital materials, and maintenance and system access logs.

5. **Monitoring Procedures**

Monitors are located in management office.

6. Viewing and Sharing Images

Live and recorded materials may be viewed by authorised operators in investigating an incident and recorded material may be downloaded from the system in line with the objectives of the scheme. Images (stills and footage) may be viewed by the Police for the detection of crime, and allowable under S*ection 29* of the *Data Protection Act (DPA) 1998*.

A written register will be used to record the release of images to the Police or other authorised applicants, maintained by authorised operators. Where images be required as evidence, a digital copy may be released to the Police; the Company retains the right to refuse permission for the Police to pass the images to any other person. The Police may require the Company to retain images for possible use as evidence in the future. Such images will be securely stored until they are needed by the Police.

Applications received from outside bodies (e.g., solicitors) to view or release images will be referred to the Directors. In these circumstances, images will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject

access request, or in response to a Court Order. A fee of £10 may be charged in such circumstances, which is appropriate for subject-access request.

7. **Retention**

Images will be retained for only as long as they are required. The system will automatically delete all recordings held on the main control unit. None of the systems enable storage after a maximum of 60 days.

In the event of a serious incident, data will be downloaded from the system and stored securely pending any external investigation. This will not be retained for longer than 60 days unless this has been deemed necessary by an external body in relation to their own investigations. As soon as it is reasonably practical the data will be deleted following any external investigation.

8. Subject Access and Freedom of Information

The *Data Protection Act* provides Data Subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV.

Requests for Data Subject Access should be made in writing to the Directors. All requests will be considered in a reasonable manner. A request for Subject Access will be charged at £10, which is the maximum allowable. A request under the *Freedom of Information Act 2000* will be accepted and responded to within 40 days, when such a request is appropriate.

9. Breaches of the Policy

Any breach of the CCTV Policy by staff members will be investigated and may result in disciplinary action, up to and including dismissal.

10. Complaints

Complaints should be addressed to the Company Directors. All complaints will be deal with following *Freedom Care Complaints Policy & Procedure.*