Community Housing

CCTV Policy

May 2024

Contents **Page**

1. Introduction

Operators of surveillance cameras are required to meet the requirements of Data Protection and ensure that in doing so they allow for individual's to retain their rights to privacy.

The unwarranted use of CCTV and other forms of surveillance cameras led to a strengthening of the regulatory landscape through the passing of the Protection of Freedoms Act 2012 (POFA). The POFA introduced specific requirements around surveillance cameras and their use.

2. Aims and objectives

The purpose of this policy is to enable all parts of SW9 to:

a) Comply with the General Data Protection Regulation (GDPR) in respect of the personal data it uses
b) Comply with the Surveillance camera code of practice (APPENDIX A)
c) Follow good data management practice;
d) Efficiently deploy and operate its surveillance systems
e) Reduce reputational risks by staying within the law and avoiding regulatory penalties
f) Help inspire trust from residents and partners in how the organisation operates CCTV
g) To ensure the use of CCTV systems across SW9 are in compliance with industry best practice

3 Policy statement

This policy applies to all employees, including any third party (this includes companies under contract with SW9) or individual, who conducts work on behalf of SW9.This policy requires compliance with the General Data Protection Regulation in relation to all Personal data (including Sensitive Personal data) that we process. This policy covers the use of camera related surveillance equipment inclusive of:

a) Unmanned aerial systems,
b) Other systems that capture information of identifiable individuals or information relating to individuals.

3.2 CCTV systems used within the organisation for the purposes of:

a) Prevention or detection of crime or disorder;
b) Apprehension and prosecution of service users (including use of images as evidence in criminal proceedings);
c) Interest of public and employee Health and Safety;
d) Protection of organisation property and assets.
e) Compliance with contractual service delivery obligations (e.g delivery of accredited programmes).

4. Performance monitoring and responsibilities

It is a condition of employment that all employees, contracted third parties and individuals abide by the policies endorsed by SW9.

Any person, who considers that this policy has not been followed in respect of Personal data relating to themselves, or others, is to raise the matter directly with their line manager, or, if the matter cannot be resolved, it can be raised as a formal grievance with the Data Protection Officer.

According to the responsibilities and activities of the role, the Data Protection officer is to ensure this policy is communicated to employees who are required to engage in CCTV use or requests as part of their role responsibilities as part of their Induction Training Program and refresher training. A formal record of all training is to be retained against the individuals' personal records.

Staff with day-to-day responsibilities for processing personal data in any form must be able to demonstrate competence in their understanding of the data protection legislation as well as being able to describe the processes through which this is implemented within the business. All staff will need to follow the CCTV Procedure.

Third party suppliers that store or process personal data on behalf of the organisation are designated Data Processors and shall be bound by a Data Processor Agreement.

Through the use of internal audit and contract monitoring, regular reviews of adherence to this policy will be undertaken; a record of such activity is to be maintained.

Any questions regarding the interpretation or operation of this policy are to be communicated to the Data Protection Officer.

5. Pre-installation assessment

SW9 recognises that its first priority under the DPA is to avoid causing harm to individuals. SW9 therefore commits to keeping information securely in the right hands and holding good quality information.

Prior to the installation of any new CCTV system, or similar surveillance equipment, within any new operating environment, SW9 will ensure to undertake an initial assessment which will be supported by a Data Protection Impact Assessment. This will include the type of personal data being processed and the purpose for which it is being captured. These DPIAs and assessments will all be stored in the same folder in Sharepoint.

SW9's CCTV systems will not be enabled for sound recording as this would not be justified in the purposes of processing.

If CCTV is deemed necessary, all cameras will be sited in prominent locations

with signs displayed in all areas where the equipment is in use. Signs will include details on the purpose for recording in that area, the organisation responsible for these systems and associated contact details.

Data subjects will also be provided with 'fair processing' information which will ensure they are fully informed of their rights and aware of the existence of CCTV cameras which may record their actions.

All camera installations and service contracts should be undertaken by approved security companies.

Images captured by CCTV systems should only be retained for a maximum 30 days, after which this information should be erased automatically, if on digital systems, or through the re-use of the relevant media on manual systems.

SW9 may operate covert CCTV. Covert CCTV will only be installed after a specialist Data Protection Impact Assessment and for a specific purpose. Its use will be regularly reviewed, and it will be removed once the issue has been resolved. Covert CCTV will not have signs.

6. Effective administration

SW9 will ensure there is a clear basis for the processing of any personal information relating to individuals that is collected from surveillance systems. Head of Customer Services has responsibility for the control of this information, for example, deciding what is to be recorded, how the information should be used and to whom it may be disclosed.

The organisation will ensure there are clearly documented procedures available to relevant staff that demonstrates how the system is to be used and best practice guidelines for handling CCTV information.

The Head of Customer Services and Head of Corporate Services are responsible for ensuring that standards are set, procedures are put in place to meet these standards, and that the system complies with GDPR requirements and best practice.

7. Third party responsibilities

Where there is another organisation involved in the CCTV processing activities, the responsibilities and obligations of each should be established firsthand. There must be clarification between the organisation and the third party about who has responsibility for control of the information and making decisions about how it can be used.

SW9 will equally ensure that its registration under the ICO clearly outlines its responsibility in the CCTV processing activities, disclosures that are made and other relevant details.

If an external organisation is providing services for processing the CCTV data, SW9 will ensure to have a sharing agreement in place which stipulates the responsibilities for data protection whilst sharing data and specifications are outlined as to how the information is to be used and security guaranteed.

8. Storing, viewing and managing surveillance system information

SW9 will ensure that recorded material is stored in a way that maintains the integrity of the information. Access will be restricted to roles that have need for the data and any further access required only authorised via the exception procedure. Viewing of live images on monitors will be restricted to the operator in the majority of situations. The organisation will endeavour to encrypt information where necessary and possible.

Recorded images can either be reviewed in our CCTV room at Park Heights or in the office or your laptop in a secure location.

All operational staff including Neighbourhood, Income, Estates and Property managers can access CCTV footage, following completion of a one-time CCTV Access form which should be submitted to the control room.

Operational staff may only access CCTV for the schemes/properties under their management, this includes schemes they are covering for a colleague. For example, an Older Person's Scheme Manager may only access the CCTV of the schemes they manage, and a Neighbourhood Officer may only view CCTV associated with the cases they are managing.

Any exceptions to this must be authorised by the respective Heads of Services. The Head of Customer Service have access to all CCTV under their service.

All areas of the business where CCTV is in operation will be required to follow the principles of the Surveillance Camera Code of Practice (Appendix A) .

9. Use of CCTV evidence and audits

The organisation will endeavour to keep a record or audit trail of the CCTV recording in the event that the information is likely to be used as evidence in court. It is important that the information is able to be used by appropriate law enforcement agencies if required. The CCTV Procedure explains the process around downloading CCTV when a resident with a crime number approaches SW9, meaning footage can be downloaded so it won't be erased after 30 days.

Access to, and the disclosure of, captured images will be tightly controlled , and is covered under our CCTV Procedure. This ensures that the rights of the individuals captured are protected and to preserve the evidential admissibility of the information gathered, should this be required.

Any individual with reasonable belief that their image has been captured by CCTV systems will be entitled to request the disclosure of these images as part of a Subject Access Request.

10. Disclosure

The disclosure of information from SW9's CCTV systems must be controlled and consistent with the purpose for which the system was established. I.e. If the system's purpose is to prevent and detect crime, then it would be appropriate to disclose to a law enforcement agency. Information in this instance must never be placed on the internet, or without full consideration of what is being done as this may cause the disclosure of the individuals' data and lead to a breach.

Note: Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose information to law enforcement agencies as failure to do so would be likely to prejudice the prevention and detection of crime.

SW9 will ensure:

a) There are arrangements in place to restrict the disclosure of information in a manner that is consistent with the purpose for establishing the system
b) Anyone who may handle requests for disclosure has clear guidance on the circumstances in which it is appropriate to make a disclosure and when it is not.
c) The date of disclosure, along with the details of who the information has been provided to is recorded.
d) Consideration is given to whether by disclosing any images of individuals, the organisation is consequently identifying the features of other individuals (there may be a need to obscure the images of others)
e) The method of disclosing is secure and that CCTV material is only disclosed to intended recipients.

11. Subject access requests

As part of the UK General Data Protection Regulation, SW9 needs to ensure individuals whose information is recorded can exercise their right of request for that information, this can be achieved by providing a copy of the footage or if they consent to it, permitting the view of that information. Further information on subject access requests is provided in the organisation's Data Protection Compliance Policy, Data Subject Rights Policy and Subject Access Request Procedure. SW9 will ensure that the Subject Access Requests processes incorporate CCTV disclosures. The design of the CCTV system must allow easy location and extraction of the personal data being requested. Redaction of third-party data must also be enabled.

Any footage requested by a resident, as part of a Subject Access Request containing other individuals must be blurred to protect their privacy.

The Head of Corporate Services will consider each CCTV SAR request on a case-by-case basis. SW9 may charge at their discretion insurance companies or third-party companies to cover the cost of blurring the footage. SW9 may also decline any request where the cost would be excessive.

SW9 would encourage any resident requesting footage in regards to a crime to first contact the police. Any footage that includes the scene of a crime but not the resident would not be considered under a Subject Access Request and could not be shown to a resident. However, we can disclose this footage to the police.

12. Enabling subject access to CCTV material

SW9's subject access procedure will incorporate the need to provide data subjects with a copy of all the information caught on CCTV material where applicable unless an exemption applies. This must be done by supplying the individual with a copy of the information in a permanent form. In particular circumstance, this obligation may not apply, e.g.:

a) Where the data subject agrees to receive their information in another way, such as by viewing the footage
b) Where the supply of a copy in permanent form is not possible or would involve disproportionate effort

If the data subject refuses an offer to view the footage or insists on a copy of the footage, then proportionate steps must be taken to provide the data subject with this information.

13. Retention

The retention of CCTV material should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose. It should not be kept for longer than is necessary as outlined in the fifth Data Protection Principle. There is no set retention limit for CCTV stemming from any regulations currently, however best practice recommends a minimum of 14 days and a maximum of 30 days retention, we will retain footage for up to 30 days. There may be instances where CCTV information may be copied onto separate discs in order to retain for longer, e.g. in the use of defence against insurance claim. Any such instances will need to be disclosed to the Data Protection officer/Head of Corporate Services.

14. Resident Use of CCTV

Residents can install CCTV within their private property. "CCTV" would include cameras as well as Ring doorbells.

Before the installation of any kind of CCTV, residents should notify Network Homes. And where required (affixing CCTV camera, other than a doorbell, to the external property) seek permission to do so as per their lease/tenancy terms.

When installing CCTV, residents must be made aware that capturing images from outside of their property means this will fall outside the scope for domestic use and they will become Data Controllers of the data. Examples of locations outside the property include: cars and pedestrians on the street, communal hallways and staircases, residents' front or back gardens.

Residents must not be operating a business from this property.

Residents must be aware that by installing CCTV they will become Data Controllers and are responsible for putting up signs, storing and disposing data securely, data should be disposed of within 1 month if they are asked to do so and shouldn't be shared with third parties and responding to Subject Access and Erasure Requests.

According to the ICO the use of recording equipment, such as CCTV or Ring door bells, to capture video or audio recordings outside the user's property boundary is not a breach of data protection law. Residents should however try and point doorbells/cameras in a way that it does not capture neighbours properties and shared spaces but this is not always possible.

The ICO provide guidance on Domestic CCTV systems (Domestic CCTV systems | ICO). Data protection law says that people who capture images or audio recordings from outside their property boundary using a fixed camera, such as a CCTV camera or smart doorbell, should:

1. Warn people that they are using recording equipment;
2. In most circumstances, provide some of the recording if asked by a person whose images have been captured;
3. Regularly or automatically delete footage;
4. In most circumstances, delete recordings of people if they ask; and
5. Stop recording a person if they object to being recorded, but only if it is possible to do so. For example, if they can point the camera in a different direction but still use it for the same purposes, e.g. keeping their property safe.

These rules do not apply to dummy cameras.

15. Accountability

Data Protection Officer **-** SW9's Data Protection Officer (DPO) is accountable for:

a) Ensuring there are appropriate controls and procedures in place to support the company to comply with current legislation relating to Data Protection and the requirements for secure systems where mass monitoring of individuals is concerned
b) Ensuring that appropriate 'fair processing' statements are made when CCTV surveillance
is undertaken
c) Ensuring that any personal data captured on CCTV systems is only obtained for specified and lawful business purposes and is not subsequently processed in a manner incompatible with those purposes (Principle 2).
d) Ensuring the business conducts periodic reviews of records to verify that the Personal data held is:
   - Adequate, relevant, and not excessive for its purpose (Principle 3);
   - Accurate and up to date (Principle 4);
   - Not kept longer than is necessary (Principle 5).
e) Ensuring that Data Subjects are able to exercise their rights (Principle 6) through the submission of a Subject Access Request for any CCTV material relating to them (where applicable)
f) Ensuring the organisation applies appropriate technical and organisational measures to safeguard against unauthorised or unlawful processing of Personal data and against any accidental loss or destruction of, or damage to Personal data (Principle 7) obtained through CCTV operating
g) Ensuring, that appropriate processes and controls exist for the disposal of CCTV data

16. Complying with this policy

Monitoring compliance - The Head of Customer Services and the Head of Corporate Services are responsible for this policy and for verifying compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and general feedback about business procedures.

Exceptions - Any exception to the policy must be raised with the Data Protection Officer in advance of exceptions taking place.

Violations/Non-Compliance - **Unauthorised disclosure of personal data is a disciplinary matter that may be considered a gross misconduct**. A violation of this Policy as well as any supporting policy documents and operating standards must be treated as an incident and investigated, the findings of which will be handled in accordance with SW9's disciplinary procedures, and could lead to termination of employment, or in the case of third parties, termination of the contractual relationship with the company; in certain circumstances this could give rise to legal proceedings.

17 Complaints

Any tenant who is dissatisfied with how we have managed their CCTV request is able to submit a complaint using our Complaints process. Once our Complaints policy is complete and if they remain dissatisfied then they can contact the Housing Ombudsman.

18. Related documents

- Data Protection Compliance Policy
- Record Management, Retention, Disposal and Archiving Policy
- Subject Access Request Procedure
- Disclosure of Personal Data to Authority Procedure
- CCTV Procedure

19. Legislation and regulation

The legislation listed in this policy is not intended to cover all legislation applicable to this policy. To meet the required RSH Governance & Financial Viability Standard outcome on adherence to all relevant law, SW9 will take reasonable measures to ensure compliance with any and all applicable legislation by reviewing policies and procedures and amending them as appropriate. The legislation listed within this policy was considered at the time of the development of this policy, but subsequent primary and secondary legislation, case law and regulatory or other requirements will be considered and the policy reviewed and adopted in accordance with the requirements set out therein, even should such subsequent legislation

not be explicitly listed within this policy. Any queries relating to the applicable legislation should be directed to the policy author.

20. Equality and diversity

We will apply this policy consistently and fairly and will not discriminate against anyone based on any relevant characteristics, including those set out in the Equality Act 2010.

21. Review

All policies should be reviewed every 3 years as a minimum, or sooner if there is a specific legislative, regulatory or service requirement or change in guidance, law or practice.

Policy author:		
Policy owner:		
Adopted from Network Homes: y/n	N	
Review schedule (1, 2 or 3 years):	3 years	
Equality Impact Assessment (EIA)	**Date completed**	
	Initial or full EIA	

Change Record

Date	Reviewed by (name and title)	Version	Summary of changes

APPENDIX A: The principles of the Surveillance Camera Code

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up

to date.