URN: TPOL019

TWENTY11 CCTV POLICY
Tenant Use of CCTV

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
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)
DPA 2018	Data Protection Act 2018
GDPR	General Data Protection Regulation

2. Purpose

2.1. This policy outlines:

2.2. How we oversee CCTV installed by our tenants at their homes.

3. Policy Statement

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

4. Tenant use of CCTV

4.1. Twenty11 does not require tenants to request permission to install CCTV at their home, including smart doorbells.

4.2. Domestic CCTV is not usually subject to data protection law, as long as this guidance is followed. Users of domestic CCTV do not need to pay a fee to the ICO and do not have to comply with the data protection requirements that a Data Controller does unless this guidance is not followed.

4.3. If the use of the CCTV goes beyond domestic use, by violating the rules explained in this guidance, the person in control of the CCTV becomes a Data Controller with legal obligations under the (UK)GDPR and DPA 2018.

4.4. Footage should only be used for household purposes, including:

- Security and safety purposes, including as a deterrent.
- Being able to see visitors at the door.
- Providing evidence to the police, for criminal investigations.
- Providing evidence to us, for ASB investigations or other tenancy breach issues.

4.5. Footage must not be published, including on social media.

4.6. Domestic CCTV should capture minimal footage in public or communal areas.

4.7. Capturing audio is more privacy-invasive than images, so audio should be kept to a minimum, and only used if absolutely necessary.

4.8. Internal CCTV should not be used to invade the privacy of visitors to the home, for example, cameras in areas such as bathrooms or toilets.

4.9. The installation of CCTV, including smart doorbells, should not cause damage to the fabric of our building(s). If such damage is caused, we may charge the tenant for the cost of repairs.

4.10. Tenants must only use CCTV footage for purely personal or household purposes.

4.11. The Information Commissioner's Office (ICO) has published guidance on the use of CCTV in domestic situations, which we have followed in our formulation of this policy and the approach we take to CCTV at tenant's homes.

5. CCTV footage shared with us

5.1. 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.

5.2. 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.

5.3. The (UK) GDPR rights of individuals that apply to CCTV include:

- The Right to Access – people can request access to their own data, which includes any footage they appear in.
- The Right to Erasure or to Object – the people in the footage can ask for it to be erased, or for us to stop using it.

Note: Some exemptions do apply when responding to these requests.

6. Equality & Diversity Statement

6.1. 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.

7. Responsibilities

7.1. Responsibility for tenant-installed CCTV lies entirely with the tenant themselves.

8. 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)

9. Sharing CCTV footage with external agencies:

9.1. All requests for access to CCTV footage which has been shared with Twenty11by a tenant will be considered in line with the GDPR Principles as above. It is key to identify a lawful basis for us to share that footage further, 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.

9.2. 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.

10. Access to images shared with us by a tenant

10.1. 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 us 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.

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

10.3. A person whose image has been recorded and retained and who wishes to have access to the data must apply in writing to the Governance team. 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

10.4. 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.

10.5. 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.

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

10.7. 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.

10.8. We hold a Data Request Register that outlines:

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

11. References

- Privacy & Data Protection Policy
- Privacy Notice

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 **Policy owner** within the applicable **delegated approvals**.

For information on interpretations and instructions staff should contact the **Subject Matter expert** or **Policy 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	**Policy owner:**	Head of Governance
Related Pod	Community	**Related Policy**	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:**	