Domestic CCTV systems/ doorbell cameras POLICY

Review lead / author name and job title.	**Ann Grimsdale, Data Protection Advisor**		
Consultation process	Housing Team, CMT review	**Distribution and training**	
Last reviewed	July 2024	**Next planned review**	July 2027
Approved by and date	Corporate Management Team 18th July 2024		
Change record.			
Version no	**Nature of change**	**Last approved**	**Approval**
1	New policy	July 2024	CMT
2			
3			
4			

Associated CHS Policies

Data Protection Policy
CCTV Policy (CHS' use of CCTV)
Tenants' Use of Surveillance Devices (in private rooms/areas of CHS facilities)
Managing Unreasonable Customer Behaviour Policy
Complaints Policy
Anti-Social Behaviour and Harassment Policy

1. Introduction and Purpose

1.1 There is an increasing number of domestic CCTV security systems, including doorbell cameras [e.g. 'Ring' doorbells]. These systems are designed to help people protect the security and safety of their homes.

1.2 CHS recognises that its customers may install such domestic CCTV systems on their properties, and that such installation can create privacy concerns among neighbours and other visitors, especially if they capture images outside of the property's boundaries.

1.3 This Policy outlines:

- the legal framework that CHS residents must comply with, if they install such a domestic CCTV system in their CHS owned/shared ownership property,
- procedures to follow if CHS residents believe they are being unfairly monitored by domestic CCTV or are in dispute about this, and
- CHS' approach, in respect of any footage captured by these systems that CHS customers submit to us as alleged evidence of anti-social or criminal behaviour

1.4 This Policy applies to you if you are a CHS tenant or shared owner/leaseholder with domestic CCTV/doorbell cameras systems at your property. When we refer to 'You' we mean CHS tenants and shared owners/leaseholders; when we refer to 'Us' we mean CHS Group.

2. Legislation

2.1 Data protection law does not apply to data collected for purely personal, family or household reasons.

2.2 However, you should be careful, especially if your domestic CCTV/doorbell camera captures images or recordings beyond your property's boundary, as you will almost certainly capture other people's images [personal data], and thus need to be mindful of their privacy rights.

2.3 As soon as your footage is used for reasons other than personal, then you will be bound by data protection law and the legal responsibilities that go with it. Non-personal use might be to harass others, or to post clips on social media. It would also include emailing footage to others (including to the police or to us) in connection with a dispute or claims of anti-social or criminal behaviour.

2.4 This means you will need to ensure your use of CCTV complies with the provisions of the UK Data Protection Act 2018, and the EU General Data Protection Regulation (GDPR).

2.5 Under such data protection law, you are the **legally responsible** controller of the data you collect on your domestic CCTV system. This means you own the recordings your CCTV system/doorbell camera makes, are legally responsible for them, and must have a justifiable reason ('lawful basis') for capturing the images in the first place. You must have considered how intrusive or upsetting these images might be to neighbours/others and what you could do to keep this to a minimum (for instance by not recording all the time or adjusting the range of the camera to capture a smaller area).

2.6 If you do not comply with your data protection obligations, you may be subject to regulatory action and/or legal action by the people whose images are captured. This could include a fine if a complaint is upheld against you, and compensation claims from those who feel their privacy had been infringed.

2.7 The Information Commissioner's Office (ICO), www.ico.org.uk is the UK's independent body set up to uphold information rights, including the data privacy rights and responsibilities of individuals.

2.8 They set out the legal rules that apply to you, if you install domestic CCTV, as follows:

11.1 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:

11.2 tell people that they are using recording equipment;

11.3 in most circumstances, provide some of the recording if asked by a person whose images have been captured;

11.4 regularly or automatically delete footage;

11.5 in most circumstances, delete recordings of people if they ask; and

11.6 stop recording a person if they object to being recorded if it is possible to do so. For example, if they can point the camera in a different direction, or use more restricted motion capture zoning, but still use it for the same purposes, e.g. keeping their property safe.

2.9 There is more guidance available on the ICO's website, https://ico.org.uk/for-the-public/domestic-cctv-systems/#rules

3. What to do if you are unhappy about someone using domestic CCTV to record you

3.1 CHS expects its customers to follow the ICO guidance https://ico.org.uk/for-the-public/domestic-cctv-systems/, namely:

13.1 ***Contact the person*** *– if you are concerned about talking to them in person, try writing them a letter.*

13.2 ***Ask why they are using CCTV*** *– people usually install domestic CCTV cameras and smart doorbells to monitor and protect personal property. They can make the user and their family feel safe. If you understand why they are recording, it may*

put your mind at ease. You might even come to an agreement where you share the system. You can then both benefit from the camera's safety features.

13.3 ***Explain your concerns*** *– the CCTV user may not understand why you are worried about being recorded. If you explain your reasons, they may change the position of the cameras.*

13.4 ***Ask to see what they are recording*** *– the footage captured by the camera may not be as intrusive as you think. Seeing an example of what the camera records may make you feel less concerned*.

3.2 Note: the steps above do **NOT** involve CHS and are **your** responsibility.

3.3 Similarly, if someone else is unhappy about you recording them, you need to ensure you follow the data protection rules set out in the ICO rules and guidance detailed in Section 2 above and are legally compliant. Again, this process does **NOT** involve CHS and is **your** responsibility.

4. What can you do if you have an ongoing dispute with a neighbour about their CCTV recording you.

4.1 If unhappiness about being recorded by CCTV cannot be resolved by following the steps in Section 3 above, there is further ICO guidance if it becomes an ongoing dispute https://ico.org.uk/for-the-public/domestic-cctv-systems/, namely:

16.1 Try to solve the problem informally by talking to them.

16.2 You could contact your landlord [in this case, CHS] to complain [and we may give you advice on handling your dispute between you]

16.3 Use a mediation service, if raising the issue informally does not work

16.4 Contact the police if your neighbour is breaking the law by being violent or harassing you.

16.5 As a last resort, take action through the courts.

4.2 ICO advice indicates that it is unlikely that the police would consider someone using CCTV to record you as harassment. However, if your neighbour is breaking the law by being violent or harassing you, you can contact CHS as well as the police.

4.3 CHS does **NOT** become involved in disagreements about the use of CCTV. This is outlined in our Anti-Social Behaviour and Harassment Policy. And, further to 16.2 above, note that CHS' Complaints Policy does **NOT** apply to things we cannot change (such as someone else's use of domestic CCTV).

5. CHS's approach to domestic CCTV recordings in support of claims made about anti-social or criminal behaviour.

5.1 If you make a claim of anti-social or criminal behaviour against someone else, CHS will follow our 'Anti-Social Behaviour & Harassment Policy'. Every case is different, and we take a case-by-case approach. As part of our approach, we might ask you if you have any legally collected CCTV recordings in support of your claim.

5.2 However, if you send us domestic CCTV recordings that you say show evidence of anti-social or criminal behaviour, CHS might **NOT** view them. This is to respect the privacy rights of all individuals concerned, and so that CHS doesn't view people's data if we aren't clear that you had a legal basis for recording the images in the first place.

5.3 If you send domestic CCTV recordings, we might:

- contact you before we decide whether to open them, to seek evidence that you are complying with data protection laws as a Data Controller and have collected the data reasonably and let us know the nature of the recording before we decide whether to view it
- view the recordings, and if we do not find evidence of anti-social or criminal behaviour, delete them, and inform you why
- delete these recordings from our system without opening them (e.g. if you repeatedly or unreasonably submit recordings)

5.4 CHS may also apply its 'Managing Unreasonable Customer Behaviour' Policy in these cases if we believe you are behaving unreasonably, making unreasonable levels of contact, or unreasonable use of the complaints process.

5.5 In certain circumstances, it may be appropriate for you to contact the police about claims of anti-social behaviour. They are responsible for dealing with antisocial behaviour that constitutes a criminal offence, for example vandalism, graffiti, or harassment. The Police will then engage with you about what records to keep supporting your claim.

FOOTNOTES: regarding mobile phones, and children's data

Footnote 1: the principles in this Policy may also apply to filming or photographing using a mobile phone. Anyone can take mobile phone footage/photographs in a public place, on streets, or from their own property for their personal use without needing permission or being subject to GDPR. But CHS will regard the use of such footage/photos in disputes, or to pursue anti-social or criminal behaviour claims as subject to the provisions of this Policy.

Footnote 2: The GDPR contains provisions intended to enhance the protection of children's personal data. They may be less aware of the risks, consequences and safeguards concerned, and of their rights. If your use of children's data falls under GDPR, you need to carefully consider the level of protection you are giving that data, and that you are behaving fairly and transparently in respect of its use.