Dunbritton Housing Association Limited

Name of Policy	**CCTV Policy**
Responsible Officer	**Head of Finance & Corporate Services**
Date approved by Board	**15 May 2024**
Date of next Review	**May 2026**
Section	**Corporate Services**
Reference	**C22**

We can produce information, on request, in large print, Braille, tape and on disc. It is also available in other languages. If you need information in any of these formats please contact us on 01389 761486

Contents.

1. Introduction

Dunbritton Housing Association (referred to herein as 'Dunbritton) owns and operates CCTV and other forms of surveillance systems at various premises. We do this for the purpose of enhancing security where we consider there to be a potential threat to the health, safety, and wellbeing of individuals and to assist in the prevention and detection of risk of crime or anti-social behaviour.

Dunbritton acknowledges the obligations it incurs in operating such systems and the rights and freedoms of those whose images may be captured. We are committed to operating them fairly and within the law at all times and in particular will comply with the requirements of the UK General Data Protection Regulations (the 'UK GDPR') and UK Data Protection Act 2018 (the 'DPA 2018').

In developing this document, Dunbritton has incorporated the standards and practices from the Information Commissioner's Office Code of Practice, 'In the picture: A data protection code of practice for surveillance cameras and personal information' as well as the Surveillance Camera Commissioner Code of Practice 'A guide to the 12 principles'.

This policy governs Dunbritton's approach to installing and operating CCTV and other forms of surveillance systems and handling the information obtained. It is underpinned by the following key principles:

- We know what the system is used for and review its use.
- That we have completed a Data Protection Impact Assessment (DPIA). Systems will only be installed with due consideration to the privacy impacts of doing so.
- That we will ensure clear signage is in place, with a published point of contact to deal with queries and complaints.
- There is clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used, and staff are aware of their responsibilities for CCTV.
- Clear rules, policies and procedures are in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- That we have a policy for keeping the CCTV images we hold, and we ensure they are deleted once they are no longer needed.
- That we have a clear process for who can access the images, and a policy on disclosure.
- That the system we use follows recognised operational and technical standards. Systems will be appropriately specified and professionally installed, having due regard to appropriate technical and legal advice and other relevant guidance.
- Systems will only be installed where there is a clear identified and documented need.
- Systems will only be installed with due consideration to all alternative options.
- Appropriate technical and organisational measures will be employed to ensure the

security of our systems and personal data, including relevant controls to govern access to and use of images.

- Appropriate measures will be taken to provide clear and accessible privacy information to individuals whose personal data is processed by systems.
- That we are clear on when CCTV images will be produced for criminal justice purposes.

This policy will be supplemented by procedures, which provide detailed operational guidance on the installation, operation, use and maintenance of our systems.

2. Decisions on Installing CCTV and Surveillance Systems

Dunbritton recognises that using CCTV and other surveillance systems can be privacy intrusive. As such it will not install systems as a routine response to incidents of a criminal or anti-social nature. Notwithstanding this, we acknowledge the potential value of these systems as both a deterrent and a means of detection and will consider all potential installations on a case-by-case basis. In doing so the aim will be to demonstrate that installation is a justified, proportionate, and effective solution to an identified problem or risk.

The impact on people's right to privacy and the availability of alternative and less intrusive options will be a key consideration. To this end, all potential installations will be subject to a Data Protection Impact Assessment (DPIA). All DPIAs will be conducted, recorded and signed off in accordance with our DPIA procedures. These have been developed in accordance with Information Commissioner's Office (ICO) guidance and prescribe the approach to be followed in identifying and assessing data protection risks, and in consulting with those whose privacy is likely to be affected, where appropriate. Dunbrittons' Data Protection Officer will advise on and review DPIAs as required.

Dunbritton will maintain a register of DPIAs as a record of decision making, installation authorisation and review. In the interests of transparency, the register and individual DPIAs shall be made publicly available on request.

3. System Specification and Installation

Dunbritton will procure and site systems in accordance with an agreed standard specification, which reflects recommended practices and incorporates privacy by design features. Relevant criteria will include, but not be limited to:

- Ensuring personal data can be easily located and extracted.
- Ensuring images are of an appropriate quality, relevant to their purpose.
- Ensuring that the date and time images are captured is easily identifiable.
- Ensuring that unnecessary images are not viewed or recorded.
- Ensuring that relevant retention periods can be complied with.
- Installing image only systems, which have no sound recording capability, as standard.

- Siting cameras to ensure only areas of interest are subject to surveillance and to minimise viewing areas not relevant to the purposes the system was installed for, with due regard given to planning permission requirements as necessary.
- Siting cameras to ensure they can produce quality images taking into account the environment where located.
- Siting cameras and equipment in secure locations, protected from unauthorised access and possible vandalism; and
- No cameras forming part of the system will be installed in a covert manner; and cameras which may be covered to protect them from weather or damage, would not be regarded as covert provided that appropriate signs are in place.

Dunbritton will engage the services of specialist contractors, in accordance with relevant procurement procedures, to advise on technical specifications and system configuration and design; and to carry out installation and maintenance. Such contractors will be required to demonstrate the appropriate credentials, expertise, and understanding of Dunbritton and data protection requirements.

Dunbritton will maintain a register of all system installations, detailing location and installation date, relevant technical specifications, and system design features.

4. Access and Use of Images

Access to all equipment and images will be strictly controlled. Appropriate security measures will be in place to ensure entry to physical locations is limited to authorised personnel. As a general rule, such authorised personnel will be individuals appointed by Dunbritton specialist contractors, acting under explicit instruction. Dunbritton will have in place a written data processing agreement with these contractors which is UK GDPR compliant and clearly defines obligations, responsibilities, and liabilities.

The specialist contractors will be responsible for setting and maintaining relevant technical security controls for each system, including passwords or access codes and for maintaining physical and digital access logs.

Dunbritton considers the following to be permitted reasons for monitoring:

- Prevention and detection of unacceptable behaviour, including aggressive or abusive actions, towards staff in Dunbritton premises.
- Prevention and detection of unauthorised access to, or other criminal activity within, Dunbritton premises; and/or
- General compliance with relevant legal obligations, regulatory requirements and Dunbritton policies and procedures.

Dunbritton shall not undertake routine monitoring of images captured in Dunbritton locations.

Access to images will be on an as required basis and in accordance with the purpose for which the system was installed. This will only be carried out where an incident has been reported that requires investigation or where there is clear suspicion that an incident has taken place. Where it is required to access or download recorded images in order to investigate an alleged incident a data request, authorised as a minimum by a member of senior management and will be recorded in the CCTV Access Register or otherwise recorded.

Access to images may also be required in order to respond to a Subject Access Request (SAR). All requests for system footage by individuals will be treated as SARs and handled in line with Dunbritton SAR Procedures. In doing so Dunbritton acknowledges the requirement to balance the rights of data subjects against those of other individuals who appear in the requested images. On receipt of a SAR, arrangements will be made to retain, and prevent automatic deletion of, all images of the individual submitting the SAR that have been captured.

The general principle will be that requests for images will be authorised as a minimum by the relevant member of senior management at Dunbritton. Images will be supplied direct to the member of senior management that authorised the request, and receipt will be logged in the CCTV Access Register or otherwise recorded. Disclosure of information from systems will be controlled and consistent with the purpose(s) for which the system was installed. As such disclosure is likely to be limited to law enforcement agencies or the Dunbritton legal advisers.

Dunbritton will not routinely keep copies of images obtained through CCTV or other surveillance systems. Any images that are returned following disclosure will be disposed of securely in accordance with Dunbritton Data Retention and Destruction Policy and Procedures.

Dunbritton considers any attempted or actual misuse of CCTV or other surveillance systems or images by staff members to be a disciplinary matter, which will be handled in accordance with the relevant policy and procedures.

Dunbritton will consider requests from Police and other legal authorities when suitable reasons have been given and that are in line with their obligations under the Investigatory Powers Act 2016. Such disclosure of information must follow our disclosure procedure.

5. Reviewing Installations

As a minimum, each system will be reviewed 6 months after initial installation and every 12 months thereafter to ensure its continued use serves a legitimate purpose and is required; and that the installation specification and design is appropriate to this purpose. This will involve a review and, as necessary, an update of the DPIA to reflect changes or actions required. Dunbritton have implemented review procedures.

Where it is determined that a system is no longer needed, arrangements for decommissioning will be made promptly. This will involve removal of all cameras and associated equipment and signage in accordance with Dunbritton CCTV and surveillance system procedures.

Notwithstanding these regular reviews, Dunbritton will separately instruct its contractors to undertake periodic maintenance and security checks. Any works to repair or replace system components, or to amend system configuration or design will be carried out only under explicit instruction.

6. Privacy Information

Dunbritton shall be as transparent as possible in its usage of CCTV and surveillance systems and Dunbritton Privacy Notices will reference the collection of personal data via systems. Clear and prominent signage will also be in place where systems are in operation. Signage requirements will be included as part of the standard system specification, and the appointed specialist contractors will be required to confirm these have been met as part of the installation process. In accordance with good practice these will state the general purpose for which the system is being used and contain relevant contact details where any enquiries should be directed. In this regard, complaints about implementation of or compliance with this Policy or the associated procedures, will be handled in accordance with Dunbrittons' Complaints Handling Procedure.

Dunbritton acknowledges that individuals also have the right to complain to the Information Commissioner's Office (ICO) directly if they feel Dunbritton is not operating CCTV and surveillance systems in accordance with the UK GDPR and/or DPA 2018.

7. Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and / or Data Protection Officer to check compliance with the law, this policy, and associated procedures. Any concerns will be raised with the Association Directors.

8. Policy Review

This policy will be reviewed every 24 months or when required, by the Data Protection Officer, to address any weakness in the procedure or changes in legislation or best practice.

Data Protection Impact Assessment

This assessment must be commenced at the beginning of any project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes must be integrated back into the project plan.

Name of Organisation	Dunbritton Housing Association
Project Title / Change Description:	CCTV Usage
Project Manager/ Lead details:	Corporate Services Officer
Name of Data Protection Officer	Claire Beckley, RGDP LLP
Date of Assessment:	8.4.24

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project scoping. Summarise why you identified the need for a DPIA.

To use CCTV externally and internally for the purposes of health and safety, the prevention and detection of crime and for the safety and security of staff, tenants, and other persons, including visitors to [insert organisation] premises.

Step 2: Describe the Processing

2a Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

We have the following CCTV cameras at the following locations:

- Surrounding of the outer building
- Within our reception area
- Within the bin shed of 6 Cronin Street

Make and Model of camera:

The footage is stored on our own internal server and is deleted continuously every 30 days.

There is live monitoring of the CCTV which is visible to staff within the Association on CCTV monitors within the office.

The data is stored internally and would only be shared with others (e.g. police / investigators / insurance companies / legal advisors) if lawful.

2b Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Details of personal data

Please indicate what personal data will be collected/stored/processed, please indicate with an X where applicable.

Video footage of individuals

Administration data

Name	☐
Date of Birth/Age	☐
Gender	☐
Contact details	☐
Unique identifier e.g. student number/NI No.	☐

Other data (please specify): **Video only**

Special Categories of data

Racial or ethnic origin	☐
Political opinion	☐
Religious or philosophical beliefs	☐
Trade Union membership	☐
Physical or mental health condition	☐
Sexual life and sexual orientation	☐
Genetic data	☐
Biometric data used to identify an individual	☐

Other sensitive information

Financial information/bank account details	☐
Criminal convictions and offences	☐

Other (please specify):

Under Article 6 of the UK GDPR one of the following conditions needs to apply before the

processing of personal data is lawful. Please indicate which condition applies:

- The individual who the personal data is about has given/will give unambiguous consented to the processing
  ☐
- The processing is necessary for the performance of a contract with the individual
  ☐
- The processing is necessary for a legal obligation
  ☐
- The processing is necessary for the vital interests of someone (i.e. life or death situation)
  ☐
- The processing is carried out in the public interest or in the exercise of official authority
  ☐
- The processing is in the legitimate interests of the business or another party and does not prejudice the rights and freedoms of the individual (please provide further details):
  ☒

If processing Special Category Data, please state which of the conditions for processing specified applies.

N/A

Video images of visitors and staff to [insert organisation].

22c Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Individuals who will be captured in the CCTV recordings will generally be staff, visitors and contractors attending the office.

People are used to having their images recorded on CCTV. The surveillance camera technology is not facial recognition CCTV.

Individuals entering and outside the premises are advised by signs that we are recording CCTV imagery. The wording of the signs reads as follows: **CCTV in operation.**

The signs are located below all of the cameras in operation.

2d Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Health and safety, security and the detection and prevention of crime.

Step 3: Consultation

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask any relevant data processors to assist? Do you plan to consult information security experts, or any other experts?

It is not deemed appropriate to carry out a consultation as all parties are aware of the requirement. The use of CCTV is covered on our Privacy Notice and there is signage in place advising of the usage, who the Data Controller is and who to contact with any concerns.

Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information

will you give individuals? How will you help to support their rights? What measures do you take to ensure data processors comply? How do you safeguard any international transfers?
The lawful basis for the processing is that it is in our legitimate interests, and we have conducted a legitimate interest assessment to that effect. It is necessary and proportionate to use CCTV recordings for the purposes stated. It is not financially practicable to employ the services of a security guard. Data is minimised through routine deletion. Individuals are made aware of the recordings through prominent signage. Data subjects can exercise their data subjects' rights in accordance with our privacy notice.

Step 5: Identify and Assess Risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of Harm	Severity of Harm	Overall risk
Interference with privacy rights	Remote	Minimal	Low

Step 6: Identify Actions to Mitigate the Risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	**Actions to reduce or eliminate risk**	**Effect on Risk** *(reduced / eliminated / Accepted)*	**Residual Risk** *(Low/ Medium/ High)*	**Action Approved** *(Yes/No)*
Risk No. 01	**Prominent signage identifying the data controller**	**Accepted**	**Low**	**Yes**

Step 7: Approval and Record of Outcomes

Item	**Signed / Date**	**Notes**
Risk Actions approved by:		*Integrate actions back*

		into project plan, with date and responsibility for completion
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
Consultation responses reviewed by:	N/A	*If your decision departs from individuals' views, you must explain your reasons*
DPO advice provided: Claire Beckley, RGDP LLP		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice: Check privacy notices are updated to refer to CCTV imagery on the legal basis of legitimate interests		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
This DPIA will be kept under review by: Corporate Services Officer		*The DPO should also review ongoing compliance with DPIA*