# Group CCTV and Surveillance Systems Policy

| POLICY IMPLEMENTATION CHECKLIST | |
|---|---|
| | |
| Policy Guardian: | Director of Finance and Governance |
| Author: | Governance Officer |
| Version number: | 1.1 |
| Approved by Chief Executive on: | December 2019 |
| Governing Body Approved: | December 2019 |
| Effective from: | December 2019 |
| Due for review on: | December 2022 |
| Diversity compliant: | n/a |
| Equality Impact Assessment required: | n/a |
| Data Protection compliant: | Yes |
| Health & Safety compliant: | Yes |
| Procedure implemented: | Yes |
| QL system changes made: | n/a |
| KPIs / reporting arrangements implemented: | n/a |
| Training Completed: | n/a |
| Posted on intranet: | January 2020 |
| Posted on website: | January 2020 |
| Publicity material issued: | n/a |
| Business Services – Implementation Review: | December 2020 |

## 1. Introduction

1.1 The Caledonia Housing Association Group (the "Group") owns and operates CCTV and other forms of surveillance systems at various premises, including offices, residential properties and community facilities, and in work vehicles. We do this for the purpose of enhancing security where we consider there to be a risk of crime or a potential threat to the health, safety and wellbeing of individuals; and to assist in the prevention and detection of criminal or anti-social behaviour.

1.2 The Group 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 General Data Protection Regulations (EU) 2016/679 (the GDPR) and UK Data Protection Act 2018 (the DPA 2018).

1.3 This policy governs the Group'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:

- 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;
- Systems will only be installed with due consideration to the privacy impacts of doing so;
- Systems will be appropriately specified and professionally installed, having due regard to appropriate technical and legal advice and other relevant guidance;
- 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;
- This policy will be supplemented by comprehensive procedures, which provide detailed operational guidance on the installation, operation, use and maintenance of our systems.

1.4 The Group recognises the increasing popularity of personal household surveillance systems and that tenants or residents may wish to install these in their homes. Without exception, the Group shall not accept any responsibility for such installations or liability for the images they capture. We will maintain appropriate procedures for responding to requests to install personal household surveillance systems.

## 2. Decisions on installing CCTV and Surveillance Systems

2.1 The Group 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.

2.2 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. The Group's Data Protection Officer will advise on and review DPIAs as required.

2.3 The Group will maintain a register of DPIAs as a record of decision making, and 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

3.1 The Group 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.

3.2 The Group 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 Group and data protection requirements.

3.3 The Group 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

4.1 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 the Group's specialist contractors, acting under explicit instruction. The Group will have in place a written data processing agreement with these contractors which is GDPR compliant and clearly defines obligations, responsibilities and liabilities.

4.2 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.

4.3 The Group considers the following to be permitted reasons for monitoring:

- Prevention and detection of anti-social and criminal behaviour or other actions which breach tenancy or occupancy agreements by residents of, or visitors to, residential properties;
- Prevention and detection of unacceptable behaviour, including aggressive or abusive actions, towards staff in office premises;
- Prevention and detection of unauthorised access to, or other criminal activity within, office premises; and/or
- General compliance with relevant legal obligations, regulatory requirements and Group policies and procedures.

4.4 Images captured in office reception areas and interview rooms will be monitored in real time by office staff during working hours in furtherance of the Group's health and safety responsibilities including its duty of care towards staff. Such staff will not have the ability to access or download recorded images. Where this is required in order to investigate an alleged incident a data request, authorised as a minimum by the relevant Operational Manager, will be submitted to the Group's specialist CCTV contractors.

4.5 The Group shall not undertake routine monitoring of images captured in residential 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. Occasional monitoring, on a short term basis may be required in order to substantiate claims of anti-social or criminal behaviour through detecting ongoing or repeated incidents.

4.6 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 the Group SAR Procedures. In doing so the Group 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.

4.7 A protocol will be in place between the Group and its contractors to govern the process for requesting copies of images and their subsequent release, storage, transportation, and destruction. This shall ensure appropriate levels of authorisation and security standards are maintained. The general principle will be that requests for images will be authorised as a minimum by the relevant Operational Manager at Caledonia; and that the contractor will similarly appoint a suitably authorised person to receive requests and instruct and approve image release. Images will be supplied direct to the Operational Manager that authorised the request, and receipt will be logged in the CCTV Access Register.

4.8 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

Group's legal advisers. The CCTV Access Register will contain relevant details of image disclosure, including named recipient and reason for disclosure.

4.9 The Group 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 the Group's Data Retention and Destruction Policy and Procedures.

4.10 The Group 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.

## 5. Reviewing Installations

5.1 As a minimum, each system will be reviewed 3 months after initial installation and every 3 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.

5.2 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 the Group's CCTV and surveillance system procedures.

5.3 Notwithstanding these regular reviews, the Group 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

6.1 The Group shall be as transparent as possible in its usage of CCTV and surveillance systems and Group Privacy Notices will reference the collection of personal data via systems. Specific communications, which signpost to the relevant Privacy Notice, will be issued by the Officer requesting the installation, to individuals likely to be affected by it. 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 the Group's Complaints Handling Procedure.

6.2 The Group acknowledges that individuals also have the right to complain to the ICO directly if they feel the Group is not operating CCTV and surveillance systems in accordance with GDPR and/or DPA 2018.

## 7. Review

7.1 This policy will be reviewed every three years or sooner if required by changes in legislation or regulatory guidance.