



## CCTV Policy

Presented for Approval by the Management Committee 27 May 2025

Next Review: May 2028

## 1. Introduction

Blochairn Housing Association (BHA) owns and operates CCTV and other forms of surveillance systems at various premises, including offices and properties. 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.

BHA 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 Regulation (the 'UK GDPR') and UK Data Protection Act 2018 (the 'DPA 2018'). In developing this document, BHA has incorporated the guidance from the Information Commissioner's Office on CCTV and Video Surveillance' as well as the Surveillance Camera Commissioner's Code of Practice 'A guide to the 12 principles'.

## 2. Purpose of the Policy

This policy governs BHA'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:

- That we know what the system is used for and review of its use;
- That we have completed a Data Privacy Impact Assessment (DPIA) and this is published on our website via the Publication Scheme. 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.

### 3. Operation of this Policy

#### 3.1 Decisions on Installing CCTV and Surveillance Systems

BHA 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. Blochairn HA Data Protection Officer will advise on and review DPIAs as required.

BHA 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.

### 3.2 System Specification and Installation

Blochairn HA 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.

BHA 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 BHA and data protection requirements.

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

### 3.3 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 BHA specialist contractors, acting under explicit instruction. BHA 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.

BHA considers the following to be permitted reasons for monitoring:

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

BHA shall not undertake routine monitoring of images captured in BHA 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 Director, will be recorded in the CCTV Access Register.

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 BHA SAR Procedures. In doing so BHA 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 Director at BHA. Images will be supplied direct to the Director that authorised the request, and receipt will be logged in the CCTV Access Register or otherwise documented.

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 BHA legal advisers. The CCTV Access Register or other documentation will contain relevant details of image disclosure, including named recipient and reason for disclosure. Any disclosure of images must be done by secure means.

BHA 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 BHA Data Retention Policy and Schedule.

BHA 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.

BHA 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.

### 3.4 Reviewing Installations

As a minimum, each system will be reviewed 6 months after initial installation and every 1 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. BHA 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 BHA CCTV and surveillance system procedures.

Notwithstanding these regular reviews, BHA 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.

## 4. Privacy Information

BHA shall be as transparent as possible in its usage of CCTV and surveillance systems and BHA 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 BHA Privacy Notices.

BHA acknowledges that individuals also have the right to complain to the Information Commissioner's Office (ICO) directly if they feel BHA is not

operating CCTV and surveillance systems in accordance with the UK GDPR and/or DPA 2018.

#### 5. Policy Review

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