Policy Name	CCTV Policy		
Policy Ref			
Review Date	September 2024		
Purpose	**REVIEW & APPROVE**		
Next Review Date	September 2027		
Committee	Service Delivery Sub Committee		
Author	Kevin Lynch		
Internal Policy	X	**To be published**	X

ANGUS HOUSING ASSOCIATION

CCTV SYSTEMS POLICY

1. Introduction

1.1 Angus Housing Association (AHA) owns and operates CCTV systems at various locations within its offices and facilities. AHA recognises its legal obligations in operating such systems and the rights and freedoms of those individuals, including its staff, service users and visitors, whose images may be captured by the systems. AHA is committed to operating CCTV systems fairly and lawfully at all times in accordance with, in particular, data protection and human rights laws.

1.2 AHA considers that CCTV systems have a legitimate role to play in helping to maintain a safe and secure environment for staff, service users and visitors, particularly in the case of CCTV systems operating within customer access areas, such as reception areas and interview rooms within AHA offices and facilities. However, AHA recognises that this may raise concerns about the effect on individuals and their privacy, as images captured of staff in this manner may constitute staff monitoring. Images captured by CCTV systems are personal data which must be handled and used by AHA in accordance with data protection and human rights laws.

1.3 This policy outlines why and how AHA uses CCTV systems, how AHA will handle and use personal data recorded by its CCTV systems, how AHA will respond to requests for disclosure of captured images and for how long AHA will retain captured images.

1.4 Responsibility for keeping this policy up-to-date and advising AHA on the use and operation of CCTV systems has been delegated to the Data Protection Officer (DPO).

2 Principles

2.1 AHA will comply with the following principles when installing and operating CCTV systems within its offices and facilities:

2.1.1 CCTV systems will only be installed and operated where there is a clear identified and documented need and legal basis for their use.

2.1.2 Privacy by design will be the principal consideration when procuring new CCTV systems or if changes are to be introduced to existing systems by way of operation or the underlying technology.

2.1.3 CCTV systems will only be installed and operated upon staff request and after a data protection impact assessment (DPIA) has been completed.

2.1.4 CCTV systems will be located to ensure that only necessary areas are captured by the systems and to not capture areas that are not relevant to the purposes for which the system has been installed, such as private homes, areas of private or neighbouring property and areas where staff

are working (to the extent that this is possible for staff working in areas where CCTV systems are in operation, such as reception areas).

2.1.5 CCTV systems will not capture sound.

2.1.6 CCTV systems will only capture images of a suitable quality for the purposes for which the systems have been installed.

2.1.7 CCTV systems will attach date and time stamps to captured images.

2.1.8 Appropriate technical and organisational measures will be put in place to ensure the security of CCTV systems and captured images and to protect the systems from vandalism. Controls will be implemented to govern access to and use of such images by authorised personnel only.

2.1.9 Appropriate measures will be taken to provide clear signage and information to individuals whose images are captured by the CCTV systems.

2.1.10 Captured images will only be retained for as long as is necessary for the purposes for which the CCTV systems have been installed.

3 Reasons for use of CCTV systems

3.1 AHA uses CCTV systems for its legitimate business purposes, including:

3.1.1 to prevent and detect (and act as a deterrent against) crime and anti-social behaviour, to protect buildings and assets from damage, disruption, vandalism and other crime and to apprehend and prosecute offenders;

3.1.2 for the personal safety of staff, visitors and other members of the public from unacceptable behaviour, including aggressive or abusive actions; and

3.1.3 to ensure general compliance with relevant legal obligations, including ensuring the health and safety of staff and others.

4 How AHA will operate CCTV systems

4.1 AHA will operate its CCTV systems, capture images and use captured images in accordance with the requirements of data protection law.

4.2 AHA will ensure that clear and prominent signs are displayed at the entrance of the area in which CCTV systems are in operation to alert individuals that their images may be captured. The signs will contain details of AHA as the organisation operating the systems, the purpose for which AHA has installed and uses the systems and contact details for further information. Supplementary information on AHA's use of CCTV systems is also available at AHA offices.

4.3 The security and integrity of captured images will be ensured by live feeds from

CCTV systems and captured images only being viewed, accessed and stored by staff who have authority to do so Where possible, monitoring screens will be positioned to prevent the public and other staff from viewing the captured images.

4.4 Staff responsible for operating the CCTV systems will exercise care when using the systems. This includes positioning CCTV system cameras so as to not overlook areas that are not intended to be captured and operating the systems sensibly, professionally and lawfully, with respect for colleagues and the general public and in accordance with this policy and applicable laws. Staff will be provided with appropriate training on the applicable laws, including on how to handle captured images securely and assist the DPO in responding to requests for captured images.

4.5 AHA will retain detailed records in situations where captured images are removed from the place that they are normally stored of:

4.5.1 date and time of removal;

4.5.2 name of the person removing the images;

4.5.3 name of the person viewing the images, including any third parties;

4.5.4 reason for removing the images (if the images were removed for use in legal proceedings, the crime incident number should be noted);

4.5.5 outcome, if any, of the removal; and

4.5.6 date and time that the images were returned to the place from which they were removed or, if not returned, whether the images were retained for evidential purposes.

5 Requests for disclosure of captured images by third parties

5.1 No images captured by AHA's CCTV systems will be disclosed to any third party, without the disclosure first being authorised by the DPO.

5.2 Images will not normally be released, unless there is demonstrable proof that they are required for crime prevention and detection, the apprehension and prosecution of offenders, legal proceedings or by court order. No captured images will be posted online or disclosed to the media.

5.3 AHA will retain detailed records of the following when disclosing captured images to third parties:

5.3.1 date and time at which access was allowed;

5.3.2 identification of any third party who was allowed access;

5.3.3 reasons for allowing access; and

5.3.4 details of the captured images to which access was allowed.

6 Individual requests for access to or erasure of captured images

6.1 Data protection law grants rights to individuals in relation to their personal data. This includes rights to request access to and erasure of their images captured by AHA's CCTV systems. Any request received must be forwarded to the DPO immediately for handling and response.

6.2 To allow AHA to handle and respond to requests and locate relevant captured images, requests must include:

6.2.1 date and time of the recording;

6.2.2 location where the images were captured; and

6.2.3 information to permit identification of the individual, if necessary.

6.3 In the case of access requests, individuals will be asked if they wish to view the captured images (if the images do not contain the images of third parties) or would like a copy. Copies will be provided on USB memory stick, unless the individual expresses an alternative preference. Viewings of captured images will take place at AHA offices where appropriate viewing facilities will be made available for this purpose.

6.4 AHA retains copyright in all images captured by its CCTV systems. Any further use or publication of images provided to an individual in response to an access request is prohibited, unless the individual obtains authorisation from AHA.

6.5 AHA is entitled to refuse access to captured images in limited circumstances, such as where disclosure would prejudice the prevention or detection of crime or the prosecution of offenders. Where captured images have been passed to the Police or Procurator Fiscal, an access request from an individual will be refused until such time as AHA has been notified that no proceedings will be taken, or proceedings have concluded.

6.6 AHA will edit, disguise or blur images of third parties when disclosing captured images in response to an access request to protect the interests of third parties captured in the images.

6.7 AHA will only erase an individual's images from captured images in response to a request where there is no legal basis or purpose for AHA to continue to hold the images. AHA will ensure that the erasure of an individual's image will not affect the images of other individuals who have been captured by the CCTV system.

7 DPIAs

7.1 AHA will complete DPIAs of existing CCTV systems at least once every 12 months to ensure that their use remains necessary and appropriate and they

continue to address the needs that justified their initial installation and operation. Where the outcome of a DPIA is that the use of a CCTV system can no longer be justified as being necessary or proportionate, arrangements for the removal of the system, together with associated equipment and signage, will be made as soon as practical thereafter.

7.2 Prior to introducing a new CCTV system, placing a CCTV system in a new location or implementing changes in how the CCTV system operates or the underlying technology, AHA will complete a DPIA to assess compatibility with the requirements of data protection law. The DPIA will assist AHA in deciding if the new system, new location or changes in operation or technology are necessary and proportionate in the circumstances, whether they should be used or if limitations should be placed on their use in the light of risks. Consideration will be given to less privacy invasive alternatives, where available.

7.3 The DPO will provide advice and assistance on DPIAs, as required.

8 Retention of captured images

8.1 Images captured by AHA's CCTV systems will be stored locally on hard disk drive and will be permanently and securely deleted after 30 days, unless continued retention is required for an ongoing issue, for example, the apprehension and prosecution of offenders or to respond to a request made by an individual under data protection law. In those situations, captured images will be retained for as long as is necessary for those purposes and steps will be taken to prevent their automatic deletion.

8.2 At the end of their useful life, hard disk drives and any physical matter, such as digital video files and hard copy prints, will be erased permanently and securely and destroyed.

9 Complaints

Complaints about the use of AHA's CCTV systems should be forwarded to the DPO in the first instance. The DPO will handle and respond to the complaints in accordance with the Complaints Policy.

10 Consequences of failure to comply

10.1 AHA takes compliance with this policy very seriously. Failure to comply with the policy:

10.1.1 puts at risk the individuals whose images are captured by the CCTV systems;

10.1.2 carries the risk of sanctions for AHA and associated significant reputational damage; and

10.1.3 may, in some circumstances, amount to a criminal offence by a member of staff.

10.2 Due to the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action for a member of staff under AHA's procedures, and this action may result in dismissal for gross misconduct.

10.3 Any questions or concerns about this policy should be directed to the DPO.

11 Review and updates to this policy

AHA will review and update this policy and may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in law.