Architectural Association School of Architecture Use of Closed-Circuit Television Systems Policy	
Version No	CCTV v0.2
Policy prepared by	Company Secretary (appointed Data Protection Manager)
Policy approved by	SMT Estates and Infrastructure group
Policy approved	
Review date	One year from above (unless prompted by legislation etc)

Business Introduction

The Architectural Association (AA), the oldest independent school of architecture in the UK, was founded in 1847 with the aspiration of 'promoting and affording facilities for the study of architecture for the public benefit'. Since 1847, the AA has been committed to producing and disseminating ideas that challenge and advance the design of contemporary culture, cities and the environment, constantly and fearlessly looking into the future.

Policy statement

The purpose of this policy is to provide direction on the use of Closed-Circuit Television (CCTV) by the AA and the circumstances in which recorded images can be retained, disclosed or deleted/destroyed.

As with any modern data gathering system, capturing images, storing, possible disclosure and eventual deletion needs to be done under controlled conditions. The AA recognises that it is essential that appropriate safeguarding measures are taken to ensure the integrity of the images captured is maintained. If images are used by the police and other law enforcement agencies, as evidence in criminal or civil trials for instance, the confidentiality, integrity and accuracy of the supplied images will need to be accepted without question.

Key risks and lawful basis for process the personal data

The Architectural Association uses CCTV on the basis that they have a legitimate interest. primarily for the prevention and detection of crime in and around the premises based in 33-38 Bedford Square, London, 1-1A Montague Street, London and Hooke Park, Dorset The key risks related to this policy are:

- Mishandling of vital evidence supporting a legal case that would render the evidence inadmissible in a court of law
- Unlawful access to images leading to a breach of confidentiality and subsequent legal action against AA

Applicability

This policy applies to all staff members (employed or contractors), students and visitors to AA's offices whose images may be captured by the CCTV system. Whilst visitors will not be expected to be familiar with this policy, signage around the company's premises must be placed such that they are in no doubt about their images will be captured by the CCTV system.

Policy details

Applicable legislation and codes of conduct

This policy takes account of all applicable legislation and guidance, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998
- CCTV Code of Practice produced by the Information Commissioner's Office

CCTV system description

There are fixed CCTV cameras situated 33-38 Bedford Square, London, 1-1A Montague Street, London and Hooke Park, Dorset of the company's premises. The precise locations are recorded and stored securely by IT / Facilities team who are responsible to the Head of Estates and Facilities.

Image recording equipment is located on the company's premises in a secure environment that is subject to strict access control. Authorised personnel only will have access to the images remotely through the provider's 'app'. Where transmitted wirelessly, all images are to be encrypted. There is to be no audio recording.

The recording equipment in use is to:

- Have the facility to isolate images such that the images of third parties can be obscured sufficiently to hide their identities
- Enable ease of viewing based on position of camera, date and time
- Allow for the transfer of images easily in response to subject access requests or requests from law enforcement agencies

An inventory of the equipment is maintained and must include as a minimum:

- Camera make, model, serial number and date of installation
- Recording equipment make, model, serial number and date of installation
- Recording medium to be itemised individually including date of first use
- Details of the person responsible for the inventory and the date of the last update

In addition, historical copies of the inventory are held and stored safely for seven years after they were updated.

CCTV camera siting

All CCTV cameras are sited in such a way as:

- To meet the purpose for which the CCTV is operated
- To be in positions where they are clearly visible to staff and visitor
- To avoid areas that are not intended to be subject to surveillance
- To absolutely avoid areas where individuals have a heightened expectation of privacy
- To avoid areas beyond the perimeter of the company premises whenever possible

Signage indicating CCTV is in use is displayed in prominent places to ensure that individuals have every chance of being made aware that a CCTV system is in operation. A siting plan is to be created and maintained by the Facilities Team and has restricted access.

Management and access

The CCTV system is to be managed by the Facilities Team but the day-to-day management of the recording equipment is to be undertaken by Head of IT. Any incidents or allegations against staff will be referred immediately to the Head of HR to determine next steps. These could include:

- Deciding who also needs to view the images
- Securing or copying the images
- Contacting the law enforcement agencies to report a possible crime

The routine viewing of live CCTV images is to be restricted the Facilities Team.

The system is maintained by an external party who have limited access……

Occasional temporary access may be granted to other members of staff but only when authorised by the Company Secretary. No other individual is to view or have access to any CCTV images unless it is in accordance with the terms of this policy.

Security features and password control

The security features of the CCTV system are set by default and are changed after due consideration of the Facilities Team and IT including the equipment provider if appropriate.

For any new equipment, the system password provided by the equipment provider is changed at the time of installation. Only those responsible for the CCTV system are

informed of the password. In the event of staff changes, the password is updated at that time.

Training

Those members of staff that are responsible for the operation and maintenance of the CCTV system are to:

- Have the appropriate technical training to perform their roles either by experienced in-house staff and/or directly from the company providing and installing the equipment
- Be familiar with the content of this policy and to confirm as much to Head of Estates and Facilities.

Image retention and storage

Any images recorded by the CCTV system are retained for only as long as necessary for the purpose for which they were originally recorded but no longer than 90 days. By exception and only when it can be justified in law, are images to be retained beyond this period. The justification must include:

- the purpose
- the appropriate lawful basis for processing
- the expected time of retention or the criteria for the extended retention
- Any restrictions on access if not specified in this policy

AA is to ensure appropriate security measures are in place such that the confidentiality, integrity and availability of the images is maintained. The measures are to include:

- Housing the recording equipment in a secure environment that is conducive to running the equipment 24/7 and that has access control.
- Transmission of CCTV images is to be protected by encryption
- Live viewing is restricted to authorised staff members only and in accordance with this policy

In addition, a log is maintained to record:

- Details of irregular access to the CCTV images, including time and dates
- Routine system maintenance to both the recording equipment and the cameras
- Any changes to the equipment itself and confirmation that the inventory has been updated
- Serviceability and quantity of media used to store images
- Notable events including equipment failure and/or loss and access requests

Disclosure in response to data subject access requests

Any individual recorded in any CCTV image has a right to request a copy of images that show themselves. When such requests are received, they are to be processed by the Data Protection Manager in the first instance and in accordance with AA's policy for handling access requests. When appropriate, the individual making the request may view the images directly on the proviso that the rights and freedoms of third parties are not adversely affected. Such a viewing is to be controlled and conducted in the company of at least one of the following:

- Head of HR
- Company Secretary
- Registrar

If it is not possible to obscure the images of third parties included in the relevant image without a disproportionate effort, then consent of these third parties should be sought prior to disclosure. If consent cannot be obtained, then the Data Protection Manager is to decide whether it is reasonable in the circumstances to disclose images i.e., where disclosures are not detrimental to the rights and freedoms of third parties that happened to be included on the images being requested

A record of all access request disclosures is to be maintained in the log and must be subject to restricted viewing to only those authorised by the Company Secretary. Details of the record are to include:

- Date of the request
- The process followed to determine whether the images contained third parties
- The factors used to determine whether images could be disclosed or accessed
- The recording of any consents or objections obtained from third parties
- Whether the images were just viewed by the individuals, when the images were viewed and in whose presence the images were viewed
- Whether a copy of the images was provided, and if so to whom, when and in what format

Disclosure in response to third party requests

AA is to disclose CCTV images to third parties when it is required to do so in accordance with data protection legislation including but not limited to sharing with police authorities or at the request of a court order. Any request for disclosure has to be justified in law.

Where there is the option to disclose images or not in response to a third party, the Senior Management Operations group is to decide, having considered the facts of the case and recommendations from Data Protection Manager in consultation with

external legal advisors where necessary. Such circumstances may include requests from the law enforcement agencies that do not have a court order.

In all circumstances where CCTV images are to be disclosed, the authorised staff are to follow the same process where possible, for the disclosure of images in response to a subject access request. From the outset, particular attention is to be paid to the precise nature and wording of the request to ensure that disclosures are restricted to that which is absolutely necessary to fulfil the request.

If there are any concerns as to disclosure then the Data Protection Manager is to be consulted in the first instance and, if required, appropriate legal advice is obtained prior to disclosures being made.

Misuse of CCTV

The misuse of CCTV equipment and/or images is a serious matter and a breach of individuals' rights and freedoms. As such it is likely to be an offence in law. Individuals suspected of such behaviour are to be subject to AA disciplinary procedures which may include reporting individuals to the police and will be gross misconduct if a disciplinary hearing finds misuse has occurred.

History

Version	Date	Reason for / summary of changes	Author
0.1	01/06/2021	First draft	DPO
0.2	16.8.23	Updating in light of internal audit review	Company Secretary