


WESTMINSTER ADULT EDUCATION SERVICE

WAES CCTV Policy

Ref No: HS5

Version: 2

Owner:	Facilities Manager	Approved by:	Executive Board	Date of approval:	11 April 2023
Effective From Date:	11 April 2023	Effective To Date:	31 July 20245	Next Review Date:	30 April 2025

 WAES VALUES – Indicate & comment on which values are attributed to this policy procedure		
Value	✓	Comment
Respect – We are inclusive and fair and strive for equality in everything we can do.	/	Static cameras will not focus on private homes, gardens and other areas of private property, staff will not direct cameras at an individual, their property or a specific group of individuals, without verbal authorisation from the Leadership Team or Facilities Manager unless an immediate response to events is required.
Aspiration – We aim high for our learners and do not accept mediocrity.		
Innovation – We strive for continuous improvement, embrace change and take risks, across all parts of the	/	Utilising digital technologies

service.		
Sustainability – We always assess our impact on the environment, whether that be physical, social or economic.	/	Recorded images will be retained for no longer than 31 days from the date of recording, unless required for evidential purposes
Excellence – In all that our staff do, they strive to be the best they can be.	/	For the security of all staff/learners/visitors etc

1. Introduction

- 1.1 Westminster Adult Education Service (WAES) is fully committed to operating a safe environment, it therefore has in place a closed-circuit television (“CCTV”) system to assist in providing a safe and secure environment for learners, staff and visitors, as well as protect WAES property.
- 1.2 CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation.
- 1.3 WAES will have due regard to the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, WAES will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein. WAES has produced this policy in line with the Information Commissioner’s CCTV Code of Practice.
- 1.4 The WAES CCTV system comprises a number of fixed and dome cameras located both internally and externally around the WAES sites. All cameras maybe monitored and are only available for use by approved members of staff.
- 1.5 The CCTV system is owned by WAES and will be subject to review on an annual basis.
- 1.6 The purpose of this Policy is to regulate the management, operation and use of the CCTV system at WAES.

2. Purpose of CCTV

2.1 WAES has installed a CCTV system:

- To increase the personal safety of staff and learners and reduce the fear of physical abuse, intimidation and crime.
- Protect WAES buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption.
- To support the Police in a bid to deter and detect crime.
- Assist in prevention and detection of crime.
- Assist with the identification, apprehension and prosecution of offenders.
- Assist with the identification of actions/activities that might result in disciplinary proceedings against staff and learners.
- Monitor security of campus buildings.

2.2 The system will be provided and operated in a way that is consistent with an individual's right to privacy.

2.3 The CCTV system will not be used to:

- Provide images to the world wide web.
- Record sound.
- Disclose to the media.

3. Responsibilities

Learners Responsibilities

3.1 It is the responsibility of all learners to:

- Be fully aware of this policy.
- Engage with their tutors in understanding its purpose and where it can be accessed.

Tutors Responsibilities

3.2 It is the responsibility of all tutors to:

- Make sure their learners are aware of this policy.
- Ensure all learners understood the purpose of this policy.
- Inform their learners of where and how to access this policy.
- Provide assurance that we are following current legislation, due diligence and Best Practice.

Managers

3.3 It is the responsibility of all managers to:

- Ensure they and their staff and/or learners understand and implement this policy
- Set examples and safeguard best practice (**refer to section 4**)
- **The Facilities Manager** is responsible for the day-to-day operation of the system and ensuring compliance with this policy.

4 Implementation - Operation.

4.1 The CCTV surveillance system is owned by WAES. The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements of the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and the Commissioner's Code of Practice.

4.2 Cameras will be used to monitor activities within the WAES buildings and other areas to identify criminal activity occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the occupants within the WAES grounds, together with its visitors.

4.3 Static cameras will not focus on private homes, gardens and other areas of private property.

- 4.4 Operators of cameras with tilt and pan and zoom capability, staff will not direct cameras at an individual, their property or a specific group of individuals, without verbal authorisation from the Leadership Team or Facilities Manager unless an immediate response to events is required.
- 4.5 Materials or knowledge secured as a result of CCTV system will not be used for any commercial purpose.
- 4.6 Downloads will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Downloads will never be released to the media for purposes of entertainment.
- 4.7 The planning and design of the existing CCTV system has endeavoured to ensure that the CCTV system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the CCTV system will cover or detect every single incident taking place in the areas of coverage.
- 4.8 Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at access routes and areas covered by the WAES CCTV System.

5 Image Viewing and Download Procedure Viewing

- 5.1 Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at access routes and areas covered by the WAES CCTV System
- 5.2 Recordings may be viewed by the police in the presence of the Leadership Team or Facilities Manager following a specific data access formal request.
- 5.3 Otherwise, permission to view CCTV data will depend on the subject of the potential investigation.
- 5.4 The Facilities Manager is authorised to review CCTV recordings to ascertain the circumstances relating to potential incidents involving learners, staff, contractors, visitors/public incidents.
- 5.5 The Facilities Manager may authorise members of the Leadership Team to view the CCTV images with them relating to a potential student incident where it may be appropriate to see the footage.
- 5.6 Potential incidents involving staff may be viewed in the presence of the Facilities Manager or Leadership Team members and overseen using the appropriate data access procedure.

Note: The Facilities Manager may take action to secure footage that may relate to an incident involving staff and others until such time that it has been decided that it is required for viewing and/or download or it can be erased.

6 Download Procedure

- 6.1 Should a download be required as evidence, an electronic copy may only be made by the Leadership Team or Facilities Manager.
- 6.2 Where this is to be released to the Police this will only be released to the Police on receipt of a completed Data Release Form and sight of their warrant card/proof of identity.

6.3 Where this is requested by a Leadership Team member relating to a student incident, a CCTV Data Release Form will be completed for the Facilities Manager.

6.4 CCTV footage may be released for civil proceedings at the written request of a solicitor or insurance company. A CCTV Data Release Form will be completed for the Facilities Manager.

6.5 All requests for downloads will be retained by the Facilities Manager for 12 months or after the incident that the download relates to has been closed.

6.6 Downloads requested by other parties and for purposes outside the scope of this policy are not permitted.

7 Breaches of this Policy

7.1 Any suspected breach of this Policy by WAES staff will be considered under the WAES's Disciplinary Policy and Procedures.

8 Overview of System

8.1 The CCTV system runs 24 hours a day, 7 days a week.

8.2 The CCTV system comprises fixed position cameras; pan tilt and zoom cameras; monitors; multiplexers; digital recorders and public information signs.

8.3 CCTV cameras are located at strategic points on site, principally at the entrance and exit point for the sites and various buildings, as well as main thoroughfares and common areas throughout the sites.

8.4 CCTV signs will be prominently placed at strategic points and at entrance and exit points of the WAES sites to inform staff, learners, visitors and members of the public that a CCTV installation is in use, its purpose and details of the operator.

8.5 Although every effort has been made to ensure maximum effectiveness of the CCTV system; it does not cover all areas and it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

9 Data Protection Act 2018

9.1 For the purpose of the General Data Protection Regulation (GDPR) the Assistant Principal Business Support Services is the designated data controller.

- CCTV digital images, if they show a recognisable person, are personal data and are covered by the General Data Protection Regulation (GDPR). This policy is associated with the WAES's GDPR Policy, the provisions of which should be adhered to at all times.
- The WAES has registered its processing of personal data (including CCTV) with the Information Commissioner's Office (ICO)

9.2 Where new cameras are to be installed on WAES premises, Part 4 of the ICO's CCTV Code of Practice will be followed before installation:

- The appropriateness of and reasons for using CCTV will be assessed and documented.
- The purpose of the proposed CCTV system will be established and documented.
- Responsibility for day-to-day compliance with this policy will be established and documented.

10 Access to Images

10.1 The General Data Protection Regulation gives individuals the right to access personal information about themselves, including CCTV images.

10.2 All requests for access to view/copy CCTV footage by individuals should be made in writing to the WAES's Facilities Manager.

Individual Access Rights

10.3 The General Data Protection Regulation gives individuals the right to access personal information about themselves, including CCTV images.

10.4 All requests for access to view/copy CCTV footage by individuals should be made in writing to the WAES's Facilities Manager.

10.5 Requests for access to CCTV images must include:

- The General Data Protection Regulation gives individuals the right to access personal information about themselves, including CCTV images.
- All requests for access to view/copy CCTV footage by individuals should be made in writing to the WAES's Facilities Manager.
- Requests for access to CCTV images must include:

10.6 The WAES will respond promptly and at the latest within 30 calendar days of receiving the request processing fee, determined by the Leadership Team and sufficient information to identify the images requested.

10.7 If the WAES cannot comply with the request, the reasons will be documented.

10.8 The requester will be advised of these in writing, where possible.

Access to Images by Third Parties

10.9 Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e., images not of the person making the request) do not have a right of access to images under the GDPR, and care must be taken when complying with such requests to ensure that neither the GDPR, HRA or the CCTV Policy are breached.

10.10 Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not have a right of access to images under the GDPR, and care must be taken when complying with such requests to ensure that neither the GDPR, HRA or the CCTV Policy are breached.

As noted above, requests from third parties will only be granted if the requestor satisfies the following criteria:

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution Agencies and their Legal Representatives.
- Insurance Companies and their Legal Representatives.

10.11 All third-party requests for access to a copy of CCTV footage should be made in writing to the WAES's Facilities Manager.

10.12 A law enforcement or prosecution agency is requesting access they should make a request in accordance with the General Data Protection Regulations.

11 Retention and Disposal

11.1 Recorded images will be retained for no longer than 31 days from the date of recording, unless required for evidential purposes or the investigation of crime or otherwise required and retained as a download with the requisite approval form.

11.2 All images on electronic storage will be erased by automated system overwriting. All downloads, still photographs and hard copy prints will be securely disposed of as confidential waste. The date and method of destruction will be recorded on the bottom of the original approval to copy held by the Facilities Manager.

12 Associated Documentation/Linked Policies/Procedures

12.1 Home Office Surveillance Camera Code of Practice

- WAES Code of Conduct.
- CCTV Code of Practice.

13 Access to the Policy

13.1 The policy will be published on the WAES SharePoint in the "Quality & Curriculum Hub" under "Policies" and the WAES website and the "Learner Hub.

14 Monitoring and Review

4.1 The Facilities Manager will review this document annually.

15 Appendices

- The Data Viewing/Release Form (SAR) (Facilities Manager) can be found at **Appendix A**



WAES Data Protection Data Viewing Form - Subject Access Request form to
Facilities Manager

S35 Data Protection Act CCTV Request

Form for completion where CCTV footage is requested under S35 of the Data Protection Act. Information required by law or made in connection to legal proceedings.

Section 1: Details of the person making the request.

Name: _____

Department: _____

Address: _____

Post Code: _____ Tel no: _____

Email Address: _____

Section 2: Details of the Leadership Team Member (if applicable)

Name: _____

Address: _____

Date of birth: _____

Section 3: Date/Time of the Incident:

Information should be provided using the 24-hour clock HH.MM i.e., 2.30 pm would be recorded as 14.30. If the precise of the incident is not known, please provide an appropriate period for the Facilities CCTV control room to locate the footage.

N.B CCTV footage is only held for **14 days** before it is overwritten on our system.

Date of Incident	Start Time HH.MM	End Time HH.MM

Section 4: What Incident the footage captured (please provide as much information as possible)

Name of Policy/Procedure	CCTV Policy
1 If Equality Impact Analysis is not relevant to this function, give reasons and proceed to section 5.	
2 In what ways could this function have a negative impact on any of the groups above? What actions have been taken to eliminate these?	Misuse – Freedom of Information Data Protection. Only to be used for legitimate interest.
3 In what ways could this function have a positive impact on any of the groups above? How will this function be used to eliminate discrimination, advance equality of opportunity and foster good relations between different groups? Are there plans for the future that will further advance equality?	Duty of Care/ Health and Safety at Work and Security Continuity.
4 What evidence supports your judgement eg. Observations, Consultations, expert opinions, quantitative or qualitative surveys. If the evidence is in the form of additional documentation where is this stored?	Followed current legislation and Best Practice

5 Has this function taken into account and cross-referenced where appropriate to Safeguarding policy and procedures? Give Details.	Due diligence, safeguarding and Data Protection.
--	--

POLICY OWNER	
Signed:	Abid Shaikh
Date:	Aug 2024

Version Control Information

Version	Date	Revision Author	Summary of Changes
1	11 April 2023	Stephen Ricked	New
2	Aug 2024	S Whitehouse/ A Shaikh	Changed front cover, extended dates as no content changes