Eastern Multi-Academy Trust
Empower - Motivate - Aspire - Transform

| | |
|---|---|
| **Policy and Procedure:** | **CCTV Policy** |
| Version: | v 1.0 |
| Author: | Alan Evans, Deputy Chief Executive |
| Approved by: | Audit Committee |
| Date of Approval: | July 2019 |
| Amended / Reviewed: | October 2019 |
| Review date: | July 2022 |

# CCTV and Surveillance Policy

At [Academy], we take our responsibility towards the safety of staff, visitors, pupils and the Academy environment very seriously. To this end, we use CCTV as part of our safeguarding to monitor any instances of aggression or physical damage to both property and people.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified. It can be used for any of the following purposes:

- Be proactive in terms of safeguarding and protection of property;
- Provide as required any substantial evidence of activities to support investigations;
- Protect individuals in relation to the use of their images and maintaining privacy.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the Academy to:

- Comply with data protection legislation, including the Data Protection Act 2018;
- Capture, and safely store for the appropriate period, video and images;
- Reassure those persons whose images are being captured, that the images are being handled in accordance with the governing data protection legislation.

This policy and its appendices should be read alongside the Covert Surveillance and Property Interference Revised Code of Practice (Code).

# Contents

1. Legal framework ..... 3
2. The data protection principles ..... 3
3. Practice ..... 4
4. Protocols ..... 4
5. Security ..... 4
6. Privacy by design ..... 5
7. Code of practice ..... 5
8. Access ..... 6
9. Roles and responsibilities ..... 7
10. Monitoring and review ..... 8

## 1. Legal framework

1.1. This policy has due regard to legislation and statutory guidance, including, but not limited to the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation (GDPR)
- The Data Protection Act (DPA) 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

1.2. This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (Data Protection Action 2018)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

## 2. The data protection principles

2.1. Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and kept up-to-date; every reasonable step will be taken so that personal data that is inaccurate will be erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that monitors appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## 3. Practice

3.1. For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- Surveillance and Audio: monitoring the movements and behaviour of individuals;
- Overt surveillance: any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000;
- Covert surveillance: any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

3.2. Covert surveillance will only be operable in extreme circumstances.

3.3. All CCTV systems shall have appropriate signage in accordance with the DPA. At [Academy] these signs will be placed on the perimeter of the CCTV system and in other strategic places.

## 4. Protocols

4.1. The surveillance system will be registered with the ICO in line with data protection legislation.

4.2. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

4.3. The surveillance system has been designed for maximum effectiveness and efficiency; however, the Academy cannot guarantee that every incident will be detected or covered and "blind spots" may exist.

4.4. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

## 5. Security

5.1. Security usage of the surveillance system, software and data will be strictly limited to authorised operators.

5.2. The Academy's authorised CCTV system operators are:

- [List operators here by role and name]

5.3. If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office authorisation forms will be completed and retained

5.4. Surveillance and CCTV systems will be tested for security flaws to ensure that they are always being properly maintained.

5.5. Surveillance and CCTV systems will never be intrusive.

5.6. Any unnecessary footage captured will be securely deleted from the Academy system or overwritten.

5.7. Each system will have a separate audio and visual system that can be run independently of one another. Audio CCTV will only be used in the case of deterring external aggressive or inappropriate behaviour. (External loudspeaker)

5.8. Any cameras that present faults will be repaired as soon as practically possible.

5.9. Visual display monitors are located [list locations of monitors].

## 6. Privacy by design

6.1. The use of surveillance cameras and CCTV will be critically analysed using a Data Protection Impact Assessment (DPIA).

6.2. A DPIA will be carried out prior to the installation of any new surveillance / CCTV system.

6.3. If the DPIA reveals any potential security risks or other data protection issues, the Academy will endeavour to have provisions in place to overcome these issues.

6.4. The Academy will make sure that the installation of the surveillance and CCTV systems will always justify its means.

6.5. If the use of a surveillance and CCTV system is too privacy intrusive, the Academy will seek alternative provision.

## 7. Code of practice

7.1. The Academy understands that recording images of identifiable individuals constitutes the processing of personal information, so it is done in line with data protection principles.

7.2. The Academy notifies all pupils, staff and visitors of the purpose for collecting surveillance data via various means including appropriate signage.

7.3. CCTV cameras are only placed where they do not negatively impact upon anyone's privacy and are necessary to fulfil their purpose.

7.4. All surveillance footage will be kept for 30 days for security purposes; the [role(s)] are responsible for keeping the records secure and allowing appropriate access.

7.5. The surveillance and CCTV system is owned by the Academy, and images from the system are strictly controlled and monitored by authorised personnel only.

7.6. The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data;
- Be transparent and include a contact point, [role of responsible contact for CCTV], through which people can access information and submit complaints;
- Have clear responsibility and accountability procedures for images and information collected, held and used;
- Have defined policies and procedures in place which are communicated throughout the Academy;
- Only keep images and information for as long as required;
- Restrict access to retained images and information with clear rules on who can gain access;
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access;
- Be regularly reviewed and audited to ensure that policies and standards are maintained;

- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement;
- Be accurate and well maintained to ensure information is up-to-date.

## 8. Access

8.1. Under the DPA 2018, individuals have the right to obtain confirmation that their personal information is being processed.

8.2. All media containing images / video belong to, and remain the property of, the Academy.

8.3. Individuals have the right to submit a Data Subject Access Request (DSAR) to gain access to their personal data.

8.4. The Academy will verify the identity of the person making the request before any information is supplied.

8.5. A copy of the information will be supplied to the individual free of charge; however, the Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

8.6. Where a DSAR has been made electronically, the information will be provided in a commonly used electronic format.

8.7. Requests by persons outside the Academy for viewing or copying CCTV media, or obtaining digital recordings, will be assessed by the Principal of the Academy, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

8.8. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged, or the request will be denied.

8.9. All fees will be based on the administrative cost of providing the information.

8.10. All requests will be responded to without delay, and almost always, within one month of receipt.

8.11. In the event of numerous or complex requests, the period of compliance may occasionally be extended by a further month. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

8.12. Where a request is manifestly unfounded or excessive, the Academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the request.

8.13. In the event that a large quantity of information is being processed about an individual, the Academy will ask the individual to specify the information the request is in relation to.

8.14. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

8.15. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law. This will be under the guidance and recommendation of the Principal:

- The police – where the images recorded would assist in a specific criminal inquiry;
- Prosecution agencies – such as the Crown Prosecution Service (CPS);
- Relevant legal representatives – such as lawyers and barristers;
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000.

8.16. Requests for access or disclosure will be recorded and the Principal of Academy will make the final decision as to whether recorded images may be released to persons other than the police.

## 9. Roles and responsibilities

9.1. [Academy], as the legal entity, is the data controller. The governing board of [Academy] therefore, has overall responsibility for maintaining records including security and access arrangements in accordance with regulations. This includes:

- Processing surveillance and CCTV footage legally and fairly;
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used appropriately;
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection;
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary;
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks;
- Ensuring that where relevant images are redacted.

9.2. The role of the data protection officer (DPO) includes:

- Dealing with freedom of information requests and DSARs in line with legislation;
- Ensuring that all data controllers at the Academy handle and process surveillance and CCTV footage in accordance with data protection legislation;
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements;
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role;
- Monitoring the performance of the Academy's DPIA for CCTV.

9.3. The role of the Principal of the Academy includes:

- Overseeing the destruction of CCTV footage when it falls outside of its retention period;
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the Academy, their rights for the data to be destroyed and the measures implemented by the Academy to protect individuals' personal information;
- Presenting reports regarding data processing at the Academy to senior leaders and the governing board;
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation;
- Monitoring legislation to ensure the Academy is using surveillance fairly and lawfully;
- Communicating any changes to legislation with all members of staff;

- Keeping records of viewing live footage (CCTV and Surveillance Policy - Appendix 2 - CCTV Log).

## 10. Monitoring and review

10.1. This policy will be monitored and reviewed on an annual basis by the DPO and the Principal of the Academy.

10.2. The Principal of the Academy will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

10.3. The Principal of the Academy will communicate changes to this policy to all members of staff.