



CCTV Policy

| | |
|--|-----------|
| Policy reviewed by Academy Transformation Trust on | June 2018 |
|--|-----------|

| | |
|--|--------------------|
| This policy links to: | Located: |
| <ul style="list-style-type: none">• Safeguarding Policy• Data Protection Policy | Website & Intranet |

Review Date – May 2019



Our Mission

To provide the very best education for all pupils and the highest level of support for our staff to ensure every child leaves our academies with everything they need to reach their full potential.

We promise to do everything we can to give children the very best education that gives them the best opportunity to succeed in life. All of our academies have it in them to be outstanding and achieving this comes down to our commitment to our pupils, staff and academies.

Our commitment

We are committed to taking positive action in the light of the Equality Act 2010 with regard to the needs of people with protected characteristics. These are age, disability, pregnancy and maternity, religion and belief, race, sex, sexual orientation, gender reassignment and marriage and civil partnership.

We will continue to make reasonable adjustments to avoid anyone with a protected characteristic being placed at a disadvantage.

We will measure the success of our commitment in this policy by analysing bullying logs and actions in our academies to reduce or eliminate incidents of bullying.

Contents

| | | |
|----|--|---|
| 1 | Policy statement | 4 |
| 2 | Purpose of CCTV | 4 |
| 3 | Description of system | 4 |
| 4 | Sitting of cameras | 4 |
| 5 | Privacy Impact Assessment | 5 |
| 6 | Management and access | 5 |
| 7 | Storage and retention of images | 5 |
| 8 | Disclosure of images to data subjects | 6 |
| 9 | Disclosure of images to third parties | 7 |
| 10 | Review of policy and CCTV system | 7 |
| 11 | Misuse of CCTV systems | 7 |
| 12 | Complaints relating to this policy | 7 |
| | Appendix 1 – CCTV Privacy Impact Assessment Template | 8 |

1 Policy statement

- 1.1 Mildenhall College Academy uses Close Circuit Television (CCTV) within the premises of the Academy. The purpose of this policy is to set out the position of the Academy as to the management, operation and use of the CCTV at the Academy.
- 1.2 This policy applies to all members of our Workforce, visitors to the Academy premises and all other persons whose images may be captured by the CCTV system.
- 1.3 This policy takes account of all applicable legislation and guidance, including:
 - General Data Protection Regulation (GDPR)
 - Data Protection Act 2018 (together with the Data Protection Legislation)
 - CCTV Code of Practice produced by the Information Commissioner
 - Human Rights Act 1998.
- 1.4 This policy sets out the position of the Academy in relation to its use of CCTV.

2 Purpose of CCTV

- 2.1 The academy uses CCTV for the following purposes:
 - To provide a safe and secure environment for pupils, staff and visitors
 - To prevent the loss of or damage to the academy buildings and/or assets
 - To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

3 Description of system

- 3.1 Bury Road
 - 3 x IP cameras, 15 Static Cameras (coax), 1 Rotating / Zoom camera (coax)
- 3.2 MCA6
 - 46x IP VR Dome Static Cameras 2.8mm – 12mm or 2.8mm Wide Angle
 - 1x IP IBT Dome Static Cameras 2.8mm – 12mm

4 Sitting of cameras

- 4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.
- 4.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The Academy will make all reasonable efforts to ensure that areas outside of the Academy premises are not recorded.
- 4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

- 4.4 Cameras will not be sited in areas where individual have a heightened expectation of privacy, such as changing rooms or toilets.

5 Privacy Impact Assessment

- 5.1 Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the Academy to ensure that the proposed installation is compliant with legislation and ICO guidance.
- 5.2 The Academy will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6 Management and access

- 6.1 The CCTV system will be managed by Susan Byles (Principal) and Marcus Skillern (Academy Manager)
- 6.2 On a day-to-day basis, the CCTV system will be operated by the Academy Manager
- 6.3 The viewing of live CCTV images will be restricted to only those authorised by the Principal or Academy Manager
- 6.4 Recorded images which are stored by the CCTV system will be restricted to access by username / password and access is restricted via a locked door.
- 6.5 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.
- 6.6 The CCTV system is checked weekly by the Academy Manager to ensure that it is operating effectively.

7 Storage and retention of images

- 7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.
- 7.2 Recorded images are stored only for a period of no more than 30 days, unless there is a specific purpose for which they are retained for a longer period.
- 7.3 The Academy will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording system being located in restricted access areas
- The CCTV system being encrypted/password protected
- Restriction of the ability to make copies to specified members of staff

7.4 Any log of any access to the CCTV images, including time and dates of access and a record of the individual accessing the images, will be maintained by the Academy.

8 Disclosure of images to data subjects

8.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation and has a right to request access to those images.

8.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of Academy Transformation Trust's Subject Access Request Policy.

8.3 When such a request is made the Academy Manager will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

8.4 If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Academy Manager must take appropriate measures to ensure that the footage is restricted in this way.

8.5 If the footage contains images of other individuals, then the Academy must consider whether:

- The request requires the disclosure of the images of individuals other than the requester (e.g. whether the images can be distorted so as not to identify other individuals)
- The other individuals in the footage have consented to the disclosure of the images, or their consent should be obtained
- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

8.6 A record must be kept, and held securely, of all disclosures which sets out:

- When the request was made
- The process followed by [insert individual with access to CCTV] in determining whether the images contained their parties
- The considerations as to whether to allow access to those images
- The individuals that were permitted to view the images and when
- Whether a copy of the images was provided, and if so, to whom, when and in what format.

9 Disclosure of images to third parties

- 9.1 The Academy will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.
- 9.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
- 9.3 If a request is received from a law enforcement agency for disclosure of CCTV images, then the Academy Manager must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.
- 9.4 The information above must be recorded in relation to any disclosure.
- 9.5 If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10 Review of policy and CCTV system

- 10.1 This policy will be reviewed annually.
- 10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed annually.

11 Misuse of CCTV systems

- 11.1 The misuse of CCTV systems could constitute a criminal offence.
- 11.2 Any member of staff who breaches this policy may be subject to disciplinary action.

12 Complaints relating to this policy

- 12.1 Any complaints relating to this policy or the CCTV system operated by the Academy should be made in accordance with the Academy's Complaints Policy.

Appendix 1 – CCTV Privacy Impact Assessment Template

1 Who will be captured on CCTV?

Pupils, staff, parents / carers, volunteers, Governors and other visitors including members of the public etc.

2 What personal data will be processed?

Facial Images, behaviour, sound etc.

3 What are the purposes for operating the CCTV system? Set out the problem that the Academy is seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

Prevention or detection of crime, damage to property, identification of unauthorised intruders etc.

4 What is the lawful basis for operating the CCTV system?

Legal Obligation, legitimate interests of the organisation to maintain health and safety and to prevent and investigate crime.

5 Who is/are the named person(s) responsible for the operation of the system?

Mrs S Byles (Academy Principal), Mr M Skillern (Academy Manager)

6 Describe the CCTV system, including:

- a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;
- b. siting of the cameras and why such locations were chosen;
- c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;
- d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and
- e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

6a. The CCTV at Bury Road & MCA6 installed systems that could capture the appropriate level of detail at the time of installation.
 6b & 6c. The cameras are located at specific high traffic areas or area that would deter crime / vandalism.
 6d. Signs have been posted on the main entrances to the sites.
 6e. The systems are not capable of 'blurring' part the image.

- 7 Set out the details of any sharing with third parties, including processors

Police, subject access, etc. Careful consideration should be given to whether any provider is used in relation to the CCTV system and the access they might have to images.

- 8 Set out the retention period of any recordings, including why those periods have been chosen

The system records 30 days of images as this provides sufficient recording time for any weekend / holiday period to be covered. This also allows for investigations to be completed without the need for moving the information off the main CCTV system.

- 9 Set out the security measures in place to ensure that recordings are captured and stored securely

All images are kept on a system that requires a username & password to access. The physical storage is a locked office with restricted access. Remote access is available (MCA6 only) and this is protected by username and strong password. This remote access is provided for maintenance purpose only.

- 10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

The CCTV is only used when authorised by either the Academy Principal or Academy Manager. This ensures it is only viewed when there is a specific need and for the specific time frame.

As the system needs a username & password to gain access this prevents any unauthorised access and reduces the risk of any data breach. The monitoring screens are always switched off when not in use and this also reduces the risk of a data breach.

Data is only transferred to third parties when authorised by the Academy Principal. The data is transferred via encrypted USB stick and only the specific time frame and camera(s) images are transferred.

11 What measures are in place to address the risks identified?

All monitoring screens are switched off
Limited access to system with user name & passwords
Physical protection of the systems – behind locked doors

12 Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

Privacy notices and public notices are displayed to inform parents, students and visitors about the use of CCTV. We have had no complaints or concerns from students or adults about the use of CCTV.

13 When will this privacy impact assessment be reviewed?

June 2019

Approval:

This assessment was approved by the Data Protection Lead:

DPL: Marcus Skillern

Date: 18/06/2019