

<b>The Cam Academy Trust Closed-Circuit Television Policy</b>	
<b>Approved in consultation with the Audit &amp; Risk Committee on behalf of the Trust Board:</b>	
<b>To be reviewed:</b>	Every 2 years or as appropriate
<b>Date of next review:</b>	April 2026
<b>Responsible Officer:</b>	C. Duckett
<b>Category - 1</b>	Version 2

### **Policy Statement**

This policy sets out the position of the Cam Academy Trust (the Trust) in relation to its use of Closed-Circuit Television (CCTV). The Trust uses CCTV at some of the school premises across the Trust. The purpose of this policy is to set out the position of the Trust as to the management, operation and use of the CCTV across the Trust and its schools.

This policy and procedures apply to all the Trust's CCTV systems, members of our workforce, visitors to the Trust our schools and all other persons whose images may be captured by the CCTV system, to ensure the Trust complies with the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and the current Information Commissions Office (ICO)code of practice.

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

- General Data Protection Regulation
- Data Protection Act 2018 (together the Data Protection Legislation)
- CCTV Code of Practice produced by the ICO
- Human Rights Act 1998
- Freedom of Information Act 2000
- The Protection of Freedoms Act 2012
- Humans Rights Act 1998

### **Purpose of CCTV**

The schools which have CCTV use it for the following purposes:

- To provide a safe and secure environment for pupils, staff and visitors (e.g. monitoring for bullying in communal areas during break times).
- Monitoring of expensive or potentially targeted areas and items (e.g. IT suite, cycle stores,) for the prevention, investigation and detection of crime.
- To prevent the loss of or damage to the school's/Trust buildings and/or assets
- To assist in the investigation of suspected breaches of school regulations and policies by staff, students or visitors.

- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.
- Monitoring the security of the site.

### **Description of system**

Some of the schools have cameras in and outside of the school building. Some cameras have sound recording capabilities and there is a range of movable and fixed cameras.

Details of the capabilities, number and location of the cameras are recorded by each school in the template which is provided at the end of this policy. If you wish to see this information for a specific school, please contact the school directly. This information is also held by the Trust Data Protection Officer.

Where a school uses cameras to record audio as well as images, such recordings will only be accessed should there be an incident of an allegation of verbal abuse or safeguarding issue. Everyday conversation of people will not be listened to.

Written authority from the designated authorised member of staff from each school is required to access audio recordings.

### **Siting of Cameras**

- 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.
- 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 school will make all reasonable efforts to ensure that areas outside of the school premises and grounds are not recorded.
- Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.
- Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilet cubicles.
- Cameras may be located in classrooms. Access to the footage is restricted and will only be used to fulfil the purposes described in the Purpose of CCTV section of this policy.

### **Privacy Impact Assessment**

- Prior to the installation or repositioning of any CCTV camera, or system, a data protection impact assessment will be conducted by the school to ensure that the proposed installation is compliant with legislation and ICO guidance. This assessment will be recorded within the Trust management system for data protection compliance called GDPR Sentry.
- Schools 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.

### **Management and Access**

- The CCTV system in each school will be the responsibility of a member of the Senior Leadership Team.
- On a day-to-day basis, the CCTV system will be operated by an individual with appropriate technical ability, usually a member of the premises team. (Designated person)
- The viewing of live CCTV images will be restricted (except for live CCTV positioned in external public areas) to the senior leadership team, designated person/s, IT management team.

(These persons will be listed in the template at the end of this policy and held by the individual school and the Trust DPO)

- Additional staff may be authorised by a senior leader of the school to monitor cameras in their own areas of responsibility on a 'view only' basis. The senior leader will ensure that the purposes described in the 'Purpose of CCTV' section of this policy are satisfied.
- Recorded images which are stored by the CCTV system will be restricted as in the above point. Relevant images may be shared with trustees or governing body panels reviewing exclusions, disciplinary matters or complaints.
- 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.
- The CCTV system is checked regularly to ensure that it is operating effectively, the images remain fit for purpose and the date and time recorded on the images is correct. The system may also need maintenance to be carried out. This will be completed by a professional company which may need access to the live recordings to ensure the system is working correctly. This would be completed in a controlled environment with a designated person present.
- All images recorded by the CCTV system remain the property and copyright of the school.
- The monitoring of staff activities will be carried out in accordance with part 3 of the ICO 'Employment Practices Code'.
- The use of covert cameras will be restricted to occasions, when a series of criminal acts or poor behaviour choices have taken place within a particular area that is not otherwise fitted with CCTV. A request for covert cameras will clearly state the purpose and reasons for use and the authority of the Head Teacher/Principal will be sought before the installation of covert cameras. All such monitoring will be fully documented and will only take place for a reasonable time.

#### **Storage and Retention of Images**

- Any images recorded by the CCTV system will be retained for no longer than 30 days unless required for evidential purposes, a SAR, the investigation of an offence, as required by law or as long as necessary for the purpose for which they were originally recorded.
- Where an image is required to be held for longer than the retention period the senior leader designated person will be responsible for authorising such a request.
- Images held more than their retention period will be reviewed on a 3 monthly basis and any information that is no longer required will be deleted.
- The school 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:

- i. CCTV recording systems being located in restricted access areas.
- ii. The CCTV system being encrypted, and password protected.
- iii. Senior leaders only to authorise copies of recordings to specified members of staff
- iv. A 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 school.

#### **Disclosure of Images to Data Subjects**

- Any individual recorded in any CCTV image is a data subject for the purposes of the data protection regulations and has a right to request access to those images.
- Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Act 2018. Such a request should be considered in the context of the Trust's Data Protection policy section - Subject Access Request.

- When such a request is made, the designated person with access to the CCTV footage will review the CCTV footage in respect of relevant time periods where appropriate, in accordance with the request.
- 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 designated person accessing the footage must take appropriate measures to ensure that the footage is restricted in this way.
- If the footage contains images of other individuals, then the school must consider whether:
  - i. The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals.
  - ii. The other individuals in the footage have consented to the disclosure of the images or their consent could be obtained
  - iii. it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
- A record must be kept within the Trust's management system called GDPR Sentry and held for all disclosures which sets out:
  - i. When the request was made.
  - ii. The process followed by the designated person with access to the CCTV footage in determining whether the images contained third parties.
  - iii. The considerations as to whether to allow access to those images
  - iv. The individuals that were permitted to view the images and the date and time when they were viewed .
  - v. Whether a copy of the images was provided and if so to whom, when and in what format.

*Note that, when a subject access request is made then unless an exemption applies (such as in relation to third party data that it would be unreasonable to disclose) then the requester is entitled to a copy in a permanent form. There is reference here only to "access" as opposed to a "permanent copy" as the school may consider it preferable in certain circumstances to seek to allow access to images by viewing in the first instance without providing copies of images. If an individual agrees to viewing the images only then a permanent copy does not need to be provided. However, if a permanent copy is requested then this should be provided unless to do so is not possible or would involve disproportionate effort.*

#### **Disclosure of Images to Third Parties**

- The school will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the data protection regulations.
- When a request for images from a third party is made to the school, the school's Data Protection Lead will be notified immediately so the process for a Subject Access Request (SAR) is followed.
- CCTV images may be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
- If a request is received from a law enforcement agency for disclosure of CCTV images, then the designated person for the CCTV footage must follow the same process as above in relation to SAR. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for. This will then enable proper consideration to be given to what can be disclosed and the potential disclosure of any third-party images. 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, the Trust Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

- The designated senior leader may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student/staff/parent discipline cases.
- A record of any disclosure made under this policy will be recorded within the Trust management system for Data protection compliance called GDPR Sentry.

### **Compliance with Data Protection Legislation**

In its administration of its CCTV system, the schools within the Trust comply with the Data Protection Act 2018 and GDPR. Regard is given to the data protection principles embodied in the Data protection Act 2018 and GDPR.

These principles require that personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not for further processes in a manner that is incompatible with those purposes
- Adequate, relevant, and limited to what is necessary in relation to the purpose for which they are processed.
- Accurate and kept up to date
- Kept in a form which permits identification of the data subjects for no longer than is necessary for the purpose for which the personal data are processed.
- Processed in a manner that ensures 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.

### **Review of Policy and CCTV System**

This policy will be reviewed every two years or earlier should the need arise.

### **Misuse of CCTV systems**

- Materials or knowledge secured because of CCTV will not be used for any commercial use or for the purpose of entertainment.
- The misuse of CCTV system could constitute a criminal offence.
- Any member of staff who breaches this policy may be subject to disciplinary action.

### **Complaints relating to this policy**

Any complaints relating to this policy or to the CCTV system operated by the school should be made in accordance with the school Complaints Policy.

Template 1

School/ college name	
The name of the designated senior leader with responsibility for the CCTV	
The name of senior leaders who have authority to view the CCTV and can give others permission to view the CCTV in their areas of responsibility.	1. 2. 3.
The name/s and job title of the designated authorised member of staff with day-to-day management of the CCTV	1. 2. 3.
Number and location of cameras (If you have a separate document with this information, it can be attached)	
Number and location of cameras that have audio	

Template 2

## **CCTV PRIVACY IMPACT ASSESSMENT TEMPLATE**

Who will be captured on CCTV?

Pupils, staff, parents / carers and other family members, volunteers, academy governors, Trust staff, contractors, emergency services personnel and other visitors including members of the public and any persons who come onto Cambourne village college site.

What personal data will be processed?

Facial Images, behaviour, movement around the school sound from the cameras that have audio

What are the purposes for operating the CCTV system? Set out the problem that the [Trust/Academy/School] 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 etc.]

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]

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

Describe the CCTV system, including:

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.

siting of the cameras and why such locations were chosen.

how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system.

where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

whether the system enables third party data to be redacted, for example via blurring of details of third-party individuals.

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. Will those processors send this data outside of the EEA, for example for storage in a cloud-based system?]

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

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

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

For example:

Is it fair to record them in the way proposed?

How is the amount of data processed to be minimised?

What are the risks of the system being accessed unlawfully?

What are the potential data breach risks?

What are the risks during any transfer of recordings, or when disclosed to third parties such as the police?

What measures are in place to address the risks identified?

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?

When will this privacy impact assessment be reviewed? – Does not need to be reviewed once agreed/authorised.

Approval:

This assessment was approved by the: Head teacher/Principal

DPO .....

Date .....

Date Recorded in GDPR Sentry .....