TOTTINGTON
HIGH SCHOOL
Excellence Through Partnership

Shaw Education Trust
We believe, you achieve

CCTV Policy

Last updated: 14 February 2020

Contents:

Statement of intent

At Tottington High School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use CCTV cameras to monitor the members of our school.

The purpose of this policy is to manage and regulate the use of the CCTV system at the school and ensure that:

- We comply with data protection legislation, including the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) – the latter of which comes into effect on 25 May 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of CCTV and other systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

For the purposes of this policy, data protection legislation refers to both the Data Protection Act 1998 and the GDPR, as both are applicable during the interim period until the GDPR comes into effect on 25 May 2018. As a result of this, this policy is compliant with the principles of both the Data Protection Act 1998 and the GDPR.

The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

1. Legal framework

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

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 1998
- 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 will also have regard to the following statutory and non-statutory guidance:

- Department for Education 'Keeping Children Safe in Education'
- Department for Education 'Working Together To Safeguard Children'
- Home Office 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- Information Commissioner's Office 'In the picture: A data protection code of practice for surveillance cameras and personal information'

1.3. This policy operates in conjunction with the following school policies:

- **School Security Policy**
- **Data Protection Policy**
- **Data Security Policy**

2. The data protection principles

2.1. Data collected from 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; further processing for archiving purposes in the public interest, scientific or historical

research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

3. Objectives

3.1. The CCTV system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils and staff.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

4. Protocols

4.1. The CCTV system will be registered with the Information Commissioner's Office (ICO) in line with data protection legislation.

4.2. The CCTV system is a closed digital system which does not record audio.

4.3. Warning signs have been placed throughout the premises to notify people that CCTV system is active, as mandated by the ICO's Code of Practice.

4.4. The CCTV system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

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

4.6. The CCTV system will not be trained on private vehicles or property outside the perimeter of the school.

5. Security

5.1. Access to the CCTV system, software and data will be strictly limited to authorised operators and will be password protected.

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

- Y Eardley Operations Manager
- M Brown Network Manager
- C Stretton Facilities Manager
- S Taylor Deputy Head
- E Guirguis Deputy Head
- J Yarwood School Principal

5.3. The main control facility is kept secure and locked when not in use.

5.4. If covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

5.5. CCTV systems will be properly maintained at all times.

5.6. Visual display monitors are located in the in the ICT office

6. Privacy

6.1. Live and recorded materials will only be viewed by authorised operators for the purpose of investigating incidents.

6.2. Images may be released to the police for the detection of crime in line with data protection legislation.

6.3. Viewings of images by the police will be recorded by Y Eardley School in a log.

6.4. Images will only be retained for as long as they are required.

6.5. Data protection impact assessments will be conducted for any new CCTV systems implemented in the school.

6.6. In the event of a data breach, the DPO will report the breach to the ICO within 72 hours if required to do so, as outlined in data protection legislation.

7. Code of practice

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

7.2. The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and emails.

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

7.4. All CCTV footage will be kept for 3 weeks for security purposes; the Principal and the ICT Manager is responsible for keeping the records secure and allowing access.

7.5. The school has a CCTV surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

7.6. The CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

7.7. The school will ensure that the CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website under the policies section.

7.8. The CCTV system will:

- Only be used for the purpose specified, which has a lawful basis.
- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point, the DPO, 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 school.
- 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 a 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, protection of pupils and staff, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

8. Access

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

8.2. All disks containing images belong to, and remain the property of, the school.

8.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

8.4. The school 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 school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

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

8.7. Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Principal, 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.

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 at the latest, within one month of receipt.

8.11. In the event of numerous or complex requests, the period of compliance will be extended by a maximum of a further two months. 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 school 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 supervisory authority and to a judicial remedy, within one month of the refusal.

8.13. In the event that a large quantity of information is being processed about an individual, the school 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 CCTV 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:

- 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 School DPO will make the final decision as to whether recorded images may be released to persons other than the police.

9. Monitoring and review

9.1. The Principal, in collaboration with the DPO, will be responsible for reviewing this policy annually.

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

9.3. The Principal will communicate changes to this policy to all members of staff.

9.4. The scheduled review date for this policy is February 2022