Closed Circuit Television (CCTV) Purpose & Code of Practice

Document Control

Version Number:	6.0
Applicable To:	All Academies
Approval Committee:	Finance & Resources
Approved:	06/07/2026
Review Cycle:	Two yearly
Date of Next Review:	September 2028
Related Policies:	Behaviour & Exclusion Policy Staff Disciplinary Policy Complaints Policy Grievance Procedure Policy

Revisions

Version	Page/Para No.	Description of Change
3	Various	Updated legislative references to UK GDPR Added Data (Use and Access) Act 2025 Other minor corrections and terminology updates

1. Statement of Intent

1.1. At the MERIDIAN TRUST, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members

1.2. The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems within the Trust schools and ensure that:

- 1.2.1. We comply with the GDPR
- 1.2.2. The images that are captured are useable for the purposes we require them for

1.3. We re-assure those persons whose images are being captured that the images are being handled in accordance with data protection legislation.

1.4. This policy covers the use of surveillance and CCTV 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:

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

2. Legal Framework

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

- 2.1.1. Data Protection Act 2018
- 2.1.2. UK General Data Protection Regulation (UK GDPR)
- 2.1.3. Protection of Freedoms Act 2012 (Sections 26–28)
- 2.1.4. Data (Use and Access) Act 2025
- 2.1.5. DfE: Protection of Biometric Information of Children in Schools and Colleges

2.2. This policy has been created regarding the following statutory and non-statutory guidance:

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

2.3. This policy operates in conjunction with the following Trust policies:

- 2.3.1. Behaviour & Exclusion Policy
- 2.3.2. Staff Disciplinary Policy
- 2.3.3. Complaints Policy
- 2.3.4. Grievance Procedure Policy
- 2.3.5. E-Safety Policy
- 2.3.6. Data Protection Policy & Privacy notices

3. Definitions

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

3.1.1. Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage

3.1.2. Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.

3.1.3. 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.

3.1.4. PIA – Privacy Impact Assessment

3.1.5. DPIA – Data Protection Impact Assessment

3.2. The MERIDIAN TRUST does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances, approved by the DPO.

4. Roles & Responsibilities

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

4.1.1. Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.

4.1.2. Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.

4.1.3. Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.

4.1.4. Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.

4.1.5. Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.

4.1.6. Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.

4.2. The MERIDIAN TRUST, as the corporate body, is the data controller. The Board of Trustees of MERIDIAN TRUST therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

4.3. The Local Senior Management team at each school will ensure that by adoption of this policy they will support the Board of Trustees fulfil their legal obligations.

4.4. The school's IT Area Manager deals with the day-to-day matters relating to data protection within their school and thus, for the benefit of this policy, will act as the data controller.

4.5. The role of the data controller includes:

4.5.1. Processing surveillance and CCTV footage legally and fairly

4.5.2. Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly

4.5.3. Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection

4.5.4. Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary

4.5.5. Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks

4.5.6. Reviewing the Surveillance and CCTV policy to ensure it is compliant with current legislation

4.6. The role of the headteacher includes:

4.6.1. Meeting with the IT Area Managers to decide where CCTV is needed to justify its means. Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.

4.6.2. Monitoring legislation to ensure the Trust is using surveillance fairly and lawfully.

4.6.3. Communicating any changes to legislation with all members of staff.

5. Purpose and Justification

5.1. The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors

5.2. Surveillance will be used as a deterrent, investigate inappropriate behaviour and damage to the school

5.3. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in any changing facilities

5.4. If the surveillance and CCTV systems fulfil their purpose and are no longer required, the school will deactivate them

6. The data protection principles

6.1. Data collected from surveillance and CCTV will be:

6.1.1. Processed lawfully, fairly and in a transparent manner in relation to individuals

6.1.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

6.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

6.1.4. Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, are erased or rectified without delay

6.1.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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.

6.1.6. 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.

7. Objectives

7.1. The surveillance system will be used to:

7.1.1. Maintain a safe environment for learning and the purposes of running an educational and recreational establishment

7.1.2. Ensure the welfare of pupils, staff, visitors and customers

7.1.3. Deter criminal acts against persons and property

7.1.4. Assist the police in identifying persons who have committed an offence

8. Protocols

8.1. The surveillance systems will be registered with the ICO in line with data protection legislation

8.2. The surveillance systems are a closed digital system

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

8.4. The surveillance 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

8.5. The surveillance systems will not be focused on individuals unless an immediate response to an incident is required

8.6. The surveillance system will not be focused on property outside the perimeter of the school

9. Security

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

9.2. The school's authorised CCTV system operators are cited in Appendix A

9.3. The school staff authorised to record and retain images are cited in Appendix A. This appendix is to be completed for each school

9.4. The main control facility is kept secure within locked equipment racks or locked rooms

9.5. If, in exceptional circumstances, covert surveillance is planned, this must have written permission from the Chief Executive Officer and the Data Protection Officer at MERIDIAN TRUST

9.6. Surveillance and CCTV systems will be tested for security flaws regularly to ensure that they are properly maintained

9.7. Surveillance and CCTV systems will not be intrusive by design

9.8. Any unnecessary footage captured will be securely deleted from the school system as specified in this policy

10. Privacy by design

10.1. The use of surveillance cameras and CCTV will be critically analysed using a PIA – under the GDPR this will become a DPIA but it will follow the same principles of a PIA.

10.2. A PIA will be carried out prior to the installation of any surveillance and CCTV system

10.3. If the PIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues

10.4. Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice

10.5. The school will ensure that the installation of the surveillance and CCTV systems will always justify its means

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

11. Code of Practice

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

11.2. The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via noticeboards, letters and signage

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

11.4. CCTV footage is not to be stored for longer than 30 days from the day it was recorded unless it is being held as part of an ongoing investigation

11.5. The school has a 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

11.6. The surveillance and CCTV system is owned by the Trust and images from the system are strictly controlled and monitored by authorised personnel only

11.7. The school will ensure that the surveillance and 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

11.8. The surveillance and CCTV system will:

11.8.1. Be designed to take into account its effect on individuals and their privacy and personal data

11.8.2. Be transparent and include a contact point, the DPO, through which people can access information and submit complaints

11.8.3. Have clear responsibility and accountability procedures for images and information collected, held and used

11.8.4. Have defined policies and procedures in place which are communicated throughout the school

11.8.5. Only keep images and information for as long as required

11.9. Restrict access to retained images and information with clear rules on who can gain access
11.10. 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
11.11. Be subject to stringent security measures to safeguard against unauthorised access
11.12. Be regularly reviewed and audited to ensure that policies and standards are maintained
11.13. 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
11.14. Be accurate and well maintained to ensure information is up-to-date

12. Access

12.1. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed
12.2. All media sources containing images belong to, and remain the property of, the Trust
12.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing
12.4. The Trust will verify the identity of the person making the request before any information is supplied
12.5. A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information
12.6. Requests by persons outside the school will be provided viewing access in conjunction with the headteacher.
12.7. Requests will be assessed by the headteacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation
12.8. CCTV access and footage will not be made available off site.
12.9. Where a request is manifestly unfounded, excessive or repetitive, the request may be denied or a reasonable fee will be charged
12.10. All fees will be based on the administrative cost of providing the information
12.11. Any CCTV information (footage) stipulated as part of a Subject Access Request must have images of all other Data Subjects (individuals) redacted. If it is not possible to redact the video footage, redacted still images may be provided. Responsibility for this rests with the Academy, however Trust IT staff will provide advice and guidance as required. Footage should only be shown after it has been viewed by the DPO to ensure that it does not contain third party information. Footage will only be shown if 3rd parties can be suitably redacted.
12.12. All requests will be responded to following the GDPR policy and associated timescales.
12.13. 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 ICO and to a judicial remedy, within one month of the refusal
12.14. 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
12.15. 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
12.16. Instances of access to recordings will be recorded in a log which can be produced on demand to the DPO, an authorised manager or Auditor/ Regulator and will be a complete record of access activity.
12.17. This log should state:
    12.17.1. dates of access
    12.17.2. the period and location covered by the recording, the reason for access and
    12.17.3. name, position and authority of those who have accessed recordings whether copies were made
12.18. 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:
    12.18.1. The police – where the images recorded would assist in a specific criminal inquiry
    12.18.2. Prosecution agencies – such as the Crown Prosecution Service (CPS) Relevant legal representatives – such as lawyers and barristers, where a court order requires it

12.18.3. 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

12.19. Requests for access or disclosure will be recorded and the headteacher will make the final decision as to whether recorded images may be released to persons other than for the purposes of law enforcement.

13. Monitoring and Review

13.1. This policy will be monitored and reviewed on a bi-yearly basis by the DPO.

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

13.3. The headteacher will communicate changes to this policy to all members of staff

Appendix A: Authorised Users Log

Please see the Trust or School website for named individuals.

For the MERIDIAN TRUST:

- The Data Protection Officer
- The Director of IT
- Executive Principals
- The Chief Executive Officer

For all schools within the trust:

- The Principal/Headteacher
- A Vice or Assistant Principal
- The IT Area Manager
- A member of the IT Technical Team (Where requested by an authorised user)

Appendix B: Record of a request to review CCTV images.

School Name _____

An Authorised member of staff must approve this request before footage is reviewed. Authorised

by: _____

Name of the person making the request to check CCTV cameras			
Date of incident			
Time of incident			
Area of school to review			
Reason for request (outline the incident that you would like the cameras checking for)			
Name of the person reviewing the recordings			
In the presence of			
Action taken	No incident identified	☒	☒
	Incident found & incident confirmed by (name)		
	Incident found & images copied or e-mailed	☒	☒

IT Technician Signed _____

Reviewer Signed _____

This form should be kept by the IT Area Manager within the IT office and available on request for auditing purposes.