FRANCIS BARBER

CCTV Policy

2025-2026

Version	DATE	DESCRIPTION
1	Jan 2026	Policy review

Reviewed date	January 2026
Responsibility	Headteacher
Committee	Premises Team
Review Date	March 2028

Contents:

Statement of intent
Legal framework
Definitions
Roles and responsibilities
Purpose and justification
The data protection principles
Objectives
Protocols
Security
Access
Monitoring and review

Statement of intent

At Francis Barber School, we take our responsibility towards the safety and security of staff, visitors, pupils and our buildings and property very seriously. To that end, we use surveillance cameras to monitor for any instances of aggression or physical damage or loss to our school and its members.

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

- We comply with data protection legislation, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).
- 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 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:

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

Legal framework

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 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

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 (GDPR)'
- 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'

This policy operates in conjunction with the following school policies:

- GDPR & Data Protection Policy
- Acceptable Use Policies
- Cyber Security Policy

Definitions

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

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.
- **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.

Francis Barber School 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 and normally only after advice from the police.

Any overt surveillance footage will be clearly signposted and will be in use in the public areas of the school.

Roles and responsibilities

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

- Providing guidance and advice on subject access requests (SAR) in line with legislation.
- Ensuring that the school 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 school's data protection impact assessment (DPIA), and providing advice where requested.

Francis Barber School, as the corporate body, is the data controller. The Management Board of Francis Barber School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The SBM deals with the day-to-day matters relating to data protection.

The role of the Administration Manager includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- 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.

The role of the Headteacher includes:

- Meeting with the DPO 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.

- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

Purpose and justification

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

Surveillance will be used as a deterrent for violent behaviour and damage and loss to the school.

The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in toilets or changing facilities. CCTV in not generally in classrooms.

The data protection principles

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.
- 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, 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.

Objectives

The surveillance system will be used to:

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

In the following locations:

- Outside the school buildings - data retention period one month
- Public areas of the school such as hall and break rooms - data retention period one month

Protocols

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

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

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

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.

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

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

Security

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

The school's authorised CCTV system operators are:

- Heads of School
- Safeguarding Leads
- Office Administrators
- Premises Manager
- School Business Manager
- Administration Manager
- IT Technician

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

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

Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times.

Surveillance and CCTV systems will not be intrusive.

Access

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

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

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

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

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. In some instances, individuals may be invited in to view their data rather than supplied with it directly. This may particularly apply to CCTV data.

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

Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, 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.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by 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.

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.

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.

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.

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 data protection legislation.

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 the police.

Monitoring and review

This policy will be monitored and reviewed on a biennial basis, or in light of any changes to relevant legislation by the DPO and the Headteacher.

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

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

The scheduled review date for this policy is March 2028.