



Surveillance and CCTV Policy

Revised: January 2019



Statement of intent

At Cardinal Allen Catholic High School, 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.

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

- We comply with the GDPR, effective 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 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

1. Legal Framework

1.1. This policy has due regard to legislation 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
- 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 has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- 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'

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

- Photography and Videos at School Policy
- E-security Policy
- Freedom of Information Policy
- GDPR Data Protection Policy

2. Definitions

2.1 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.

2.2 Cardinal Allen 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.

2.3 Any overt surveillance footage will be clearly signposted around the school.

3. Roles and Responsibilities

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

- Ensuring that all data controllers at 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.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- 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.
- Monitoring the performance of the school's data protection impact assessment (DPIA) and providing advice where requested.

3.2 Cardinal Allen Catholic High School, as the corporate body, is the data controller. The governing board of Cardinal Allen Catholic High School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3 The SBM deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

3.4 The role of the data controller 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.

3.5 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.

4. Purpose and Justification

- 4.1 The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors.
- 4.2 Surveillance will be used as a deterrent for violent behaviour and damage to the school.
- 4.3 The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.
- 4.4 If the surveillance and CCTV systems fulfil their purpose and are no longer required the school will deactivate them.

5. The data protection principles

- 5.1 Data collected from surveillance and CCTV will be:
- Processed lawfully, fairly and in a transparent manner in relation to individuals.
 - Adequate, relevant and limited to what is necessary in relation to the purposes for which they 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.

6. Objectives

- 6.1 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.

7. Protocols

- 7.1 The surveillance system will be registered with the ICO in line with data protection legislation.
- 7.2 The surveillance system is a closed digital system which does not record audio.
- 7.3 Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.
- 7.4 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.
- 7.5 The surveillance system will not be trained on individuals unless an immediate response to an incident is required.
- 7.6 The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

8. Security

- 8.1 Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.
- 8.2 The school's authorised CCTV system operators are:
- Andrew Cafferkey, Headteacher.
 - Jane Abra, DPO.
 - Julian Addington-Barker, data processor.
 - Jake Bannister, data processor.
- 8.3 The main control facility is kept secure and locked when not in use.
- 8.4 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.
- 8.5 Surveillance and CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times.

- 8.6 Surveillance and CCTV systems will not be intrusive.
- 8.7 The DPO and headteacher will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders.
- 8.8 Any unnecessary footage captured will be securely deleted from the school system.
- 8.9 Each system will have a separate audio and visual system that can be run independently of one another. Audio CCTV will only be used in the case of deterring aggressive or inappropriate behaviour.
- 8.10 Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.
- 8.11 Visual display monitors are located in the IT technical office and the headteacher's office.

9. Privacy by Design

- 9.1 The use of surveillance cameras and CCTV will be critically analysed using a DPIA, in consultation with the DPO.
- 9.2 A DPIA will be carried out prior to the installation of any surveillance and CCTV system.
- 9.3 If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.
- 9.4 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.
- 9.5 The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

10. Code of Practice

- 10.1 The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- 10.2 The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.
- 10.3 CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- 10.4 All surveillance footage will be kept for One month for security purposes; the headteacher and the Senior IT Technician are responsible for keeping the records secure and allowing access.
- 10.5 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.
- 10.6 The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.
- 10.7 Be accurate and well maintained to ensure information is up-to-date.

11. Access

- 11.1 Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.
- 11.2 All disks containing images belong to, and remain the property of, the school.
- 11.3 Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing. Please see our GDPR Data Protection Policy.
- 11.4 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
- 11.5 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.

12. Monitoring and Review

- 12.1 This policy will be monitored and reviewed on an annual basis by the DPO and the headteacher.

- 12.2 The DPO will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.
- 12.3 The headteacher will communicate changes to this policy to all members of staff.

Cardinal Allen Catholic High School

Melbourne Avenue, Fleetwood. FY7 8AY

www.cardinalallen.co.uk

head@cardinalallen.co.uk

01253 872659

@CardinalAllen