

ST PETER'S CHURCH OF ENGLAND PRIMARY SCHOOL, HARBORNE

SURVEILLANCE & CCTV POLICY

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 Data Protection Regulation Act 2018
- The Freedom of Information Act 2000
- Human Rights Act 1998
- 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 operates in conjunction with the following school policies:

- Photograph and Videos at School Policy
- Privacy Notice
- Safeguarding Policy
- Freedom of Information Policy
- 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 St Peter's Church of England Primary 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.

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

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system.

Cameras are located in: the external areas of the school grounds – playgrounds, gates and entrances, together with roof areas on both sites.

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance.

Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

3. ROLES AND RESPONSIBILITIES

- 3.1 St. Peter's Church of England Primary School as the corporate body, is the data controller. The governing body of St Peter's Church of England Primary School, therefore, has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.2 The Governing Body

The Governing Body has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in Section 2.1) is complied with.

3.3 The Head Teacher

The Head Teacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of the data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties.

3.4 The Data Protection Officer

The Data Protection Officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Train all staff to recognise a subject access requests
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed with it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Receive and consider requests for third-party access to CCTV footage

3.5 The Site Manager

The Site Manager will

- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly

3.6 The School Business Manager 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.

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
- 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.

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.
- 7.7 The CCTV system will be operational 24 hours a day, 365 days a year
- 7.8 The system is registered with the Information Commissioner's Office
- 7.9 The system will not record audio
- 7.10 Recordings will have date and time stamps. This will be checked by the site manager termly and when the clocks change.

8. SECURITY

- 8.1 Access to the surveillance system, software and data will be strictly limited to authorised operators.
- 8.2 The school's authorised CCTV system operators are:
 - Mrs A Leonard, Head Teacher
 - Mrs L James, Deputy Head Teacher
 - Mrs K Bass, Deputy Head Teacher
 - Mrs M Easley, DPO/School Business Manager
 - Mr B Easley, Site Manager
- 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 (**Appendix A**) 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 Head Teacher 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 school office on both sites.

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

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 eight days for security purposes; the Head Teacher and the data controller 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 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 website.
- 10.8 The surveillance and CCTV system will:
- 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 the surveillance and 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 purpose for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.

10.9 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 discs containing images belong to, and remain the property of, the school.
- 11.3 Individuals have the right to submit subject access request SAR to gain access to their personal data in order to verify the lawfulness of the processing.
- 11.4 The school will verify the identity of the person making the request before any information is supplied.
- 11.5 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.
- 11.6 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- 11.7 Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Head Teacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.
- 11.8 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- 11.9 All fees will be based on the administrative cost of providing the information.
- 11.10 All requests will be responded to without delay and at the latest, within one month of receipt.
- 11.11 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.
- 11.12 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 ICO and to a judicial remedy, within one month of the refusal.
- 11.13 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.

- 11.14 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 the individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.
- 11.15 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 enquiry.
 - 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
- 11.16 Requests for access or disclosure will be recorded and the Head Teacher will make the final decision as to whether recorded images may be released to persons other than the policy.

12. MONITORING & REVIEW

- 12.1 This policy will be monitored and reviewed on an annual basis by the DPO and the Head Teacher.
- 12.2 The Head Teacher will be responsible for monitoring any changes to legislation that may affect the policy, and make the appropriate changes accordingly.
- 12.3 The Head Teacher will communicate changes to this policy to all members of staff.