CCTV Policy

Holy Trinity CofE Primary School

Version 5

Date of last review:	September 2024
Date of this review:	September 2026
Date of next review:	September 2028

Contents

+

Introduction	3
Objectives of the CCTV Policy	3
Statement of Intent	4
The Data Protection Principles	5
Operational Controls and Protocols	5
Monitoring Procedures	7
Recorded Material Procedures	7
Record Keeping/Incidents Log	8
Retention of Data	8
Security	8
Data Protection Impact Assessment (DPIA)	9
Breaches of the Policy	9
Assessment of the CCTV System	9
Access by the Data Subject	9
Complaints & Contact Details	10

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at Holy Trinity CofE Primary School, hereafter referred to as 'the school.

The CCTV system is maintained by Site Watch and monitored by MV Tech.

On a day-to-day basis, cameras are monitored by Site Manager. Recorded images from any camera can only be accessed with express permission from either the Head Teacher.

The systems will not be used for any other purpose other than those set out in this document without prior consultation with the Head Teacher and where appropriate, notification to staff.

This Policy has been drafted in compliance with the requirements of the General Data Protection Regulation, hereafter referred to as GDPR.

The ongoing suitability of the Schools CCTV Policy will be reviewed annually by the School Governing Body.

The system is registered with the Information Commissioners Office (ICO)

2. Objectives of the CCTV Policy

This Policy covers the use of CCTV systems on the school site, which capture moving and still images of people who could be identified, for the following purposes;

- To protect school buildings, and their assets within
- To increase personal safety of those within, and visiting the school community
- To act as a deterrent for violent behaviour and damage to the school
- To support the Police in a bid to deter and detect crime.
- To assist in identifying, apprehending and disciplining offenders

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

- Information Commissioner's Office (ICO) (2024) 'Video Surveillance (including guidance for organisations using CCTV)'
- Biometrics and Surveillance Camera commissioner (Gov) (2022) Update to Surveillance Camera Code of Practice - GOV.UK (www.gov.uk)

This policy has due regard to legislation including, but not limited to, the following:

- The General Data Protection Regulation

- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Protection of Freedoms Act 2012
- The Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- The Schools Standards and Framework Act 1998
- The Equality Act 2010
- The Children Act 2004
- European Convention of Human Rights

This policy operates in connection with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Safeguarding Policy
- Privacy notices for Pupils, Parents and Carers
- Privacy Notice for School Staff
- Privacy Notice for Visitors and Contractors

3. Statement of Intent

The school will treat the system, and all information, documents and recordings obtained and used as data, which are protected by the GDPR, and will be processed in accordance with the requirements of the regulation.

The lawful basis for processing personal data via a CCTV system is Article 6(1)(e) of the UK General Data Protection Regulation (UK GDPR); processing is necessary for the performance of a task carried out in the public interest. This includes safeguarding pupils, staff and visitors; maintaining school security; preventing and detecting crime; and protecting school property.

Cameras will be used to monitor activities within allocated areas around school; to identify criminal activity occurring, anticipated or perceived, and in order to ensure the safety and wellbeing of the school community. Images may be viewed and evidenced as part of investigating incidents/perceived incidents.

The school recognises that CCTV footage may include images of children and therefore operates the system with regard and care to its safeguarding duties. CCTV will only be used where it is necessary and proportionate, and in a manner that is consistent with the best interests of children; the school safeguarding obligations; and applicable data protection legislation.

The school will only operate overt surveillance and will display signs in the areas of the school where this is in operation. Warning signs have been placed at all access routes to areas covered by the school CCTV, as required by the Code of Practice of the Information Commissioner. The school does not routinely

undertake covert surveillance. More information is available in section 6: Monitoring procedures.

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

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

CCTV cameras will not be installed in areas where individuals would have a reasonable expectation of privacy, including toilets, changing facilities or similar areas. If CCTV is installed in areas where privacy is required (such as union meetings), the school will ensure recordings are not viewed or retained.

4. The Data Protection Principles

Data collected from CCTV will be processed in accordance with the principles of the GDPR. As such, all data will be:

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

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

(c) Adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed.

(d) Accurate and where necessary, kept up to date.

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

(f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

5. Operational Control & Protocols

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

The CCTV system will be in operation for 24 hours a day, 365 days a year. The system will not record audio.

The responsibility of the day-to-day leadership and management of the CCTV system is that of the Head Teachers.

The system will be managed by the Site Manager in accordance with the principles and objectives expressed in this Policy.

The day-to-day administration of the system will be the responsibility of the Site Manager during the day, out of hours and at weekends.

The CCTV system will be operated by motion sensors 24 hours a day, every day of the year.

The Operational Controller will check and confirm the efficiency of the system and in particular, to confirm that the equipment is properly recording and that cameras are functional.

The System Administrator will ensure that **all** staff involved with the operation of the CCTV system are properly trained and fully understand their roles and responsibilities in respect of data protection e.g.:

- the user's security policy (procedures for access to recorded images;
- the user's disclosure policy;
- rights of individuals in relation to their recorded images.
- Training records will be maintained accordingly.

Access to the CCTV 'viewing monitors' will be limited to selected administrative staff together with those directly involved in the security of the school.

Staff, visitors and others entering areas with CCTV viewing monitors will be subject to particular arrangement as outlined below.

Authorised staff will satisfy themselves over the identity of visitors to the area and the purpose of their visit. Where any doubt exists, the CCTV monitors will be switched off for the duration of visit.

Operations of the equipment will be managed with the minimum of disruption. Casual observations will not be permitted.

If an emergency arises out of hours, permission will be obtained from The Head Teacher - to view or process recorded material.

Other operational functions will include maintaining recorded materials and hard disc space, filing and maintaining occurrence and system maintenance logs.

Incidents involving the Emergency Services will be notified to the Head Teacher.

Where third-party suppliers are used to maintain, support, store or host CCTV systems, appropriate contractual and data processing arrangements will be in place to ensure compliance with UK data protection legislation.

6. Monitoring Procedures

Camera surveillance may be maintained at all times.

Pictures will be continuously recorded or when activated by movement.

The school does not routinely undertake covert surveillance. Any exceptional use of covert monitoring would only be considered in the most serious circumstances, where it has been deemed as lawful, necessary and proportionate. To do so, authorisation is required from the Headteacher in consultation with the school Data Protection Officer and safeguarding leads where appropriate. The rationale, scope and duration of covert monitoring will be fully documented.

7. Recorded Material Procedures

In order to maintain and preserve the integrity of the recorded material used to record events from the CCTV system, and the facility to use them in any future proceedings, the following procedures for their use and retention **will** be strictly adhered to:

(a) Each item of recorded material will be identified by a unique mark.

(b) The system will register the date and time of recorded material insert, including recorded material reference.

(c) Any recorded material required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure recorded material store. If recorded material is not copied for the Police before it is sealed, a copy may be made at a later date, it will then be resealed, witnessed, signed by the Controller, dated and returned to the evidence material store.

(d) If the recorded material is archived the reference will be noted.

Recorded materials may be viewed by / released to third parties, only in the following prescribed circumstances, and then only to the extent required by law:

- The police, where any 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;
- Insurance companies where images may be required to process a potential liability claim.
- Persons whose images have been recorded and retained, and where disclosure is required by virtue of data protection legislation, or the Freedom of Information Act.

A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register, maintained by the Controller will be made available for this purpose.

Viewing of recorded materials by the Police will be recorded in writing and in a log book.

Recorded materials will be released to the Police but will remain the property of the school, and both the recorded material and information contained on it are to be treated in accordance with this document.

The school retains the right to refuse permission for the Police to pass to any other person, the recorded material or any part of the information contained thereon.

Upon a court of law request the release of an original recorded material will be produced from the secure recorded material store, complete in its sealed bag.

If the Police require the school to retain the stored recorded materials for use as evidence in the future, such recorded materials will be properly indexed and properly and securely stored until they are required by the Police.

Requests for access or disclosure will be recorded and the Head Teacher will make the final decision as to whether the recorded images may be released to persons other than the police.

8. Record Keeping / Incident Logs

The school will maintain adequate and comprehensive records relating to the management of the system and incidents. Model documents from the installers/providers of CCTV system may be utilised for this purpose.

9. Retention of Data

There are no specific guidelines about the length of time data images should be retained. Consequently, the period of retention will be determined locally, will be documented and understood by those operating the system and will be for the minimum period necessary to meet the objectives of the CCTV scheme. A period of 30 days is considered adequate unless determined otherwise.

Measures to permanently delete data will be clearly understood by persons that operate the system.

Systematic checks will be carried out to ensure the appropriate retention periods are adhered to and footage is deleted in line with the retention policy.

Where CCTV data is required to assist in the prosecution of a criminal offence, data will need to be retained until collected by the Police.

10. Security

All devices used are encrypted so that CCTV footage is stored securely at all times. Access to footage will be via password by authorised personnel only.

Security measures are in place to protect all footage from potential cyber-attacks.

11. Data Protection Impact Assessments

Where changes to the CCTV system are made such as additional cameras being installed or moved to other areas on site, or a complete replacement, a Data Protection Impact Assessment (DPIA) will be carried out. This will identify potential risks to data by replacing or developing the system as well as to ensure the system remains justifiable, necessary and proportionate in line with the GDPR.

The schools DPO will provide guidance and appropriate paperwork required to capture proposals and considerations made and to identify potential risk and safeguards needed. The completion of the DPIA will be led by the School Business Manager.

12. Breaches of the Policy (including breaches of security)

Any breach of the policy by school staff will be initially investigated by the head Teacher to determine appropriate action, if necessary, and to make recommendations on how to remedy the breach in liaison with the schools Data Protection Officer.

13. Assessment of the CCTV System

An annual assessment will be undertaken by the Site Manager to evaluate the effectiveness of the CCTV system.

The outcome of the assessment will be reported to the Schools Governing Body who will determine if the system is achieving the objectives of the scheme, or if modifications are required.

14. Access by the Data Subject

The UK General Data Protection Regulation (UK GDPR) gives individuals the right to access personal data held about them by the school, including personal data recorded by CCTV systems.

Individuals, or those with parental responsibility acting on behalf of a child where appropriate, may submit a Subject Access Request (SAR) to obtain copies of CCTV footage in which they are identifiable.

CCTV footage may contain images (and therefore the personal data) of more than one identifiable individuals. In such cases, the school will consider whether disclosure can be made by redacting or obscuring the images of third parties, or whether an exemption under data protection legislation applies.

Where the school is unable to provide a copy of CCTV footage because the footage contains images of other individuals and effective redaction is not technically possible, the school may consider offering the requester a supervised viewing of the footage. In some circumstances, the school may also provide a written description of the relevant footage instead of providing a copy. Each request will be assessed on its own merits and in accordance with UK GDPR, safeguarding obligations and the rights of third parties.

The school will not disclose footage where doing so would:

- adversely affect the rights and freedoms of others;
- prejudice the prevention or detection of crime;
- compromise safeguarding arrangements;
- where another lawful exemption applies.

The school will take reasonable steps to verify the identity of the individual making the request, and where applicable, their authority to act on behalf of another individual, before releasing any information.

All requests will be responded to without undue delay and, in any event, within one calendar month of receipt, unless an extension is permitted under data protection legislation.

In line with procedures, requests for access/disclosure of CCTV will be recorded. The Headteacher, or other authorised individual, will make a final decision regarding the release of recorded images, seeking advice from the Data Protection Officer where appropriate.

15. Complaints and Contact Details

In the first instance concerns, questions or complaints should be directed to the Data Protection Lead at office.manager@holytrinity.sandwell.sch.uk. This includes if a data subject wishes to make a Subject Access Request, is concerned about a data breach or has general queries in relation to data protection within the school.

If a data subject requires further assistance after contacting the Data Protection Lead, this should then be discussed with the Data Protection Officer who can be contacted at:

Email: gdpr@sips.co.uk

Telephone number: 0121 296 3000.

After contacting the Data Protection Lead and Data Protection Officer, if a data subject remains dissatisfied with the assistance that they have received, they can make a formal complaint to the Information Commissioners Office.

The Information Commissioner can be contacted at:
Information Commissioners Office, Wycliffe House Water Lane Wilmslow Cheshire, SK9 5AF

Tel: 0303 123 1113
Website: https://ico.org.uk