

# CCTV Policy

## St Peter's Catholic Primary School

Lichfield Rd, Bloxwich, Walsall WS3 3LY

[www.st-peters.walsall.sch.uk/](http://www.st-peters.walsall.sch.uk/)



### MISSION STATEMENT:

Learning Together

Loving God

Becoming the best I can

Last reviewed on: November 2025

Next review due by: November 2026

## Contents

1. Introduction.....	3
2. Lawful Processing.....	3
3. Objectives of the CCTV Scheme.....	3
4. Roles and Responsibilities.....	4
5. Operation of the System.....	5
5.1 CCTV Control / Monitors.....	5
6. Siting of Cameras.....	5
7. Covert Surveillance.....	6
8. Notification – Signage.....	6
9. Storage and Retention of Recorded Images.....	7
9.1 Storage.....	7
9.2 Retention.....	7
9.3 Procedure for Exporting Recorded Events from CCTV System.....	8
10. Disclosure of Images.....	8
10.1 Requests by the Police.....	8
10.2 Subject Access Requests (Right to Access).....	9
10.3 Freedom of Information.....	9
11. Breaches of the Procedures (including security breaches).....	10
12. Monitoring and Review.....	10
13. Complaints.....	11

## **1. Introduction**

The purpose of this policy and procedure is to provide assistance in the operation, management and regulation of the CCTV system in place at St Peter's Catholic Primary School.

These procedures follow the ICO 'Code of Practice for Surveillance Cameras and Personal Data' the Data Protection Act 2018 (DPA) guidelines and the Data Protection Policy which is available to view on the school website.

### **1.1 Exemptions**

The use of cameras (non-surveillance) for domestic purposes is exempt from the Data Protection Act. e.g. a video taken by parents of pupils participating in school performances (Christmas/drama productions, etc.), school sports events recorded for the parent/carer's own family use and not published on social media.

The use of cameras or other recording devices (not CCTV) by the news media or for artistic purposes, such as for film making, are not covered by these procedures as an exemption within the DPA applies to activities relating to journalistic, artistic and literary purposes.

## **2. Lawful Processing**

St Peter's Catholic Primary School has responsibility for the safeguarding of children and staff who are present onsite under the requirements of Keeping Children Safe In Education (statutory guidance). The school owes a duty of care under the provisions of the Health and Safety at Work etc. Act, 1974 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment to support these responsibilities.

The use of CCTV by the school where footage recorded includes the identifiable personal data (images only) is undertaken in line with the conditions of the Data Protection Act 2018 (UKGDPR) and Data Use and Access Act 2025.

In implementing and using CCTV, the school has also considered its responsibilities under the following legislation:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- Keeping Children Safe In Education 2024
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- Children Act 2004
- Equality Act 2010

This procedure outlines the school's use of CCTV and how it complies with relevant data protection legislation.

We have considered the privacy issues involved with using surveillance systems and have concluded that their use is necessary and proportionate to needs that we have identified. We have also considered less privacy intrusive methods of achieving this need where possible. The use of CCTV to control the perimeter of the school buildings and entrances/exits for security purposes has been deemed to be justified by the Board of Governors.

## **3. Objectives of the CCTV Scheme**

The system comprises of 12 fixed cameras located both externally and internally for the purpose of capturing images of intruders or of individuals damaging property or removing goods without authorisation and/or instances of poor behaviour, for example. CCTV systems will not be used to monitor normal behaviour in school.

School CCTV systems will be used for the following purposes:

- protecting the school building and assets, both during and after hours.
- increasing the personal safety of staff, pupils and visitors.
- supporting statutory safeguarding responsibilities.
- reducing the fear of crime.
- reducing the risk of bullying.
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Police in a bid to deter and detect crime.
- assisting in identifying, apprehending and prosecuting offenders.
- protecting members of the public; and
- ensuring that the school rules are respected so that the school can be properly managed.

#### **4. Roles and Responsibilities**

The Data Protection Officer will be responsible for monitoring compliance with these procedures.

The Headteacher is responsible for all day-to-day leadership around data protection matters in school.

All authorised operators and employees with access to CCTV images will be made aware of these procedures prior to access being granted to CCTV systems. All operators have also received training in appropriate use of the system in relation to their data protection responsibilities. In particular, they have been made aware of:

- What the school's arrangements are for recording and retaining information
- How to handle the information securely
- How to recognise a subject access request and what to do if they receive one
- What to do if they receive a request for information from an Official Authority, for example, or the Police. (See point 10.1)

The school's authorised CCTV system operators are:

- Headteacher
- Data Protection Officer
- Office Manager, School Business Manager
- Designated Safeguarding Lead
- Members of the school SLT

Monitoring for security purposes will be conducted in a professional, ethical and legal manner. Any use of CCTV systems for other purposes is strictly prohibited.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with existing policies adopted by the school including the Data Protection Policy.

Our procedures for video monitoring prohibits monitoring based on the characteristics and classifications contained in the Equalities Act 2010 and other related legislation, for example race, gender, sexual orientation, national origin, disability etc. The system is in place to monitor suspicious behaviour and not individual characteristics.

CCTV monitoring of public areas for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by Law.

Cameras will be used only to monitor activities around the external areas, our car park and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the Staff, Pupils and visitors.

Staff have been instructed that cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals. This should only take place where an authorisation from an Official Authority is obtained to justify Directed Surveillance, as set out in the Regulation of Investigatory Power Act 2000 (RIPA).

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police.

The planning and design has endeavoured to ensure that the surveillance scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the ICO Code of Practice have been placed at all access routes to areas covered by CCTV.

Information obtained through the CCTV system may only be released to third parties when authorised by either the Headteacher or the Data Protection Officer. Any requests for CCTV recordings/images from the Police will be logged by the school and the Data Protection Officer. If a law enforcement authority is seeking a recording for a specific investigation, any such request made should be made in writing.

## **5. Operation of the System**

- The CCTV system life cycle will be managed by the school, in accordance with the principles and objectives expressed within these procedures.
- The day-to-day management of the system availability will be the responsibility of the Site Manager during the day, out of hours and at weekends.
- The CCTV system will be operated 24 hours each day, every day of the year.

### **5.1 CCTV Control / Monitors**

Viewing of live images on monitors are usually restricted to the operator and any other authorised person where it is necessary for them to see it, e.g. to monitor access/egress points around the site.

Recorded images are reviewed using cloud-hosted software accessible to named users who have been provisioned with user accounts to the system.

The monitoring or viewing of images from areas where an individual would have an expectation of privacy are restricted to authorised personnel.

- The Site Manager will check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.
- Staff who have access to CCTV software, must ensure that sessions are locked if devices are left unattended
- Other administrative functions will include maintaining CCTV footage and maintaining and system maintenance logs.
- Emergency procedures will be used in appropriate cases to call the Emergency Services.

## **6. Siting of Cameras**

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify.

The school has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers- by or of another person's private property.

CCTV video monitoring and recording of public areas may include the following:

- **Protection of school buildings and property:** The building's perimeter, entrances and exits.
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas.
- **Video Patrol of Public Areas:** Parking areas, main entrance/exit gates.
- **Criminal Investigations (carried out by the Police):** Robbery, burglary and theft surveillance.

The following points were considered when the CCTV cameras were installed:

- Camera locations were chosen carefully to minimise viewing spaces that are not of relevance to the purposes for which we are using CCTV.
- The cameras have been sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed.
- Cameras are suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera.
- We have checked that a fixed camera positioned in winter will not be obscured by the growth of plants and trees in the spring and summer.
- Cameras are sited so that they are secure and protected from vandalism.
- The system will produce images of sufficient size, resolution and frames per second.

## **7. Covert Surveillance**

The school will not engage in covert surveillance.

Certain law enforcement agencies may request to carry out covert surveillance on the school premises. Such covert surveillance may require a Court Order. Accordingly, any such request made by law enforcement agencies will be requested in writing. The covert surveillance activities of public authorities are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type of recording is covert and directed at an individual or individuals.

## **8. Notification – Signage**

The school will provide a copy of these CCTV Procedures on request to staff, students, parents/carers and visitors. These procedures describe the purpose and location of CCTV monitoring, and contact details for those wishing to discuss CCTV monitoring and guidelines for its use.

The school is required to notify individuals when they are in an area where a CCTV system is in operation. The most effective way of doing this is by using prominently placed signs at the entrance to the system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the CCTV systems are very discreet, or in locations where people might not expect to be filmed. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a CCTV system.

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the school property.

Where CCTV is in operation, signs will:

- Be clearly visible and readable
- Be an appropriate size



All staff will be made aware of what to do or who to contact if a member of the public makes an enquiry about the surveillance system.

## **9. Storage and Retention of Recorded Images**

### **9.1 Storage**

Recorded material will be stored in a way that maintains the integrity of the information on the CCTV systems hard drive. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose.

The system will be stored in a secure environment on hard disk with automatic logs of access to the images created. Access will be restricted to authorised personnel as above. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by the Data Protection Officer and other individuals in order to achieve the objectives set out above e.g. the Police, the School. Business Manager, other members of the teaching staff, representatives of the Department for Education (DfE), representatives of the Health and Safety Executive (HSE). When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

The school will keep a record or audit trail showing how the information must be handled if it is likely to be used as evidence in court. Once there is no reason to retain the recorded information, it will be deleted. Exactly when we decide to do this will depend on the purpose for using the surveillance systems. A record or audit trail of this process will also be captured.

CCTV images are digitally recorded. It is important that our information can be used by appropriate law enforcement agencies if it's required. In this event, a copy will be made onto a removable drive and handed to the Police.

### **9.2 Retention**

The Data Protection Act 2018 does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose.

The Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. As a data controller, the school needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a calendar month (30 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue. It will be overwritten automatically as the disk space is used up.

### 9.3 Procedure for Exporting Recorded Events from CCTV System

In order to maintain and preserve the integrity of the Data used to record events from the CCTV hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to.

#### Internal Use

- Exported images should be saved to a CCTV folder on the staff shared area with restricted access to certain members of staff.
- The file name should contain the date, time of incident
- A reference should be noted in the CCTV Log book.
- The exported clip should be deleted when no longer required.

#### For External Use

- An appropriately secure method should be used for transferring data externally.
- Any discloses made using removeable media that are required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored securely.

## 10. Disclosure of Images

Information captured by the CCTV systems is highly likely to constitute personal data, including special category data. Decisions to disclose this information externally may only be made by the Headteacher of the academy or the Governing Board in consultation with the Data Protection Officer.

Requests will be considered on a case-by-case basis but such information may be disclosed to:

- the Police in order to support the detection and prevention of crime;
- the Health and Safety Executive, Local Authority, or any other statutory body charged with safeguarding children and young people in order to promote that safeguarding;
- individuals (or their authorised representatives) in response to a subject access request for their own personal data or where the requested information is subject to a court order; or
- the academy's insurance provider, where the information is required to support a claim for damages done to the insured property.

Where information is requested by an external organisation, or an individual as an information rights request, this request should be made in writing. All requests will be reported to the DPO and logged by the System Operator.

In many cases, where the personal data of multiple individuals is captured, the academy in consultation with the Data Protection Officer will be responsible for determining whether the disclosure of CCTV footage as part of an information rights request is reasonable.

The academy's current CCTV system does not support the redaction of live or exported footage.

The Data Protection Officer will consider whether disclosure of footage can be achieved in a manner that protects the rights and privacy of other individuals whose personal data may be contained in any clip/section of footage. Where disclosure of live/raw footage is not possible, the academy must consider whether the disclosure of still images taken from footage will allow an information rights request to be upheld.

### 10.1 Requests by the Police

Information obtained through video monitoring will only be released when authorised by the Headteacher following consultation with the Data Protection Officer. If the Police request CCTV images for a specific investigation, any such request made by the Police should be made in writing.

- Data may be viewed by the Police for the prevention and detection of crime, authorised officers of the Local Authority for lawful statutory purposes.

- The lawful purpose for requesting CCTV footage should be identified in any requests received by the Police
- A record will be maintained of the release of Data to the Police or other authorised applicants. A log will be available for this purpose.
- Viewing of Data by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under Part 3 of the Data Protection Act 2018
- Should images be required as evidence, a copy may be released to the Police under the procedures described previously in this Code.
- The Police may require the school to retain the stored Data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the Police.
- Applications received from outside bodies (e.g. solicitors) to view or release data will be referred to the Data Protection Officer. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

Once we have disclosed information to another body, such as the Police, they become the Data Controller for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures.

## 10.2 Subject Access Requests (Right to Access)

Staff involved in operating the surveillance system have been trained to recognise a subject access request. A log of the requests received will be kept and how they were dealt with.

Individuals whose personal data has been captured on the school CCTV system has the right to request a copy of their personal data from information recorded.

Any request of this nature will be referred immediately to the Data Protection Officer for advice. All requests too access CCTV footage will be reviewed to determine whether such an image/recording exists i.e. has not been deleted and whether the data can be disclosed without the application of another exemption/prohibition.

Reasonable and proportionate searches will be conducted where a request relates to CCTV footage. If the scope of the request is not clear at the point of submission, the school or DPO may require the request to be clarified. It is reasonable for the school to request further information about specific dates, times and locations of cameras before responding to a subject access request.

Where the image/recording identifies other individuals, the school will only disclose footage where it can be redacted/anonymised. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be disclosed. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or is exempt from disclosure.

In giving a person a copy of their data, the school may provide a still/series of still pictures, or an export with relevant images. However, any images of other individuals will be redacted (obscured) before the data is released.

When making a request, a person should provide all the necessary information to assist the school in locating the CCTV recorded data, such as the date, time and location of the recording.

To exercise their right of access, a data subject can email the Data Protection Officer directly [DPO@st-peters@wasall.sch.uk](mailto:DPO@st-peters@wasall.sch.uk)

The school will respond to requests **within 30 calendar days** of receipt.

## 10.3 Freedom of Information

The school may receive requests under the Freedom of Information Act (FOIA). The school will respond to Freedom of Information requests within 20 working days from receipt of the request.

Section 40 of the FOIA contain a two-part exemption relating to information about individuals. If we receive a request for surveillance system information, we will consider:

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA. Instead this request should be treated as a data protection right of access request.
- Is the information personal data of other people? If it is, then the information can only be disclosed if this would not breach the data protection principles.

In practical terms, if individuals are capable of being identified from the CCTV system, then it is personal information about the individual concerned. It is generally unlikely that this information can be disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the DPA.

## **11. Breaches of the Procedures (including security breaches)**

- Any breach of these procedures by school staff will be initially investigated by the Data Protection Officer, in order for him/her to take the appropriate disciplinary action.
- Any serious breach of the procedures will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.
- Information obtained in violation of these procedures such as covert surveillance may not be used in a disciplinary proceeding against an employee of the school, or a pupil.

## **12. Monitoring and Review**

Routine performance monitoring, including random operating checks, may be carried out by the Headteacher, Site Manager or Data Protection Officer.

These procedures will be regularly reviewed by the Data Protection Officer. This is to ensure the standards established during the setup of the system are maintained.

Similarly, there will be a periodic Governing Board review, of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified. The review will take into account the following:

- Is it addressing the needs and delivering the benefits that justified its use?
- Is information available to help deal with queries about the operation of the system and how individuals may make access requests?
- Does the information include our commitment to the recommendations in the ICO Code of Practice and include details of the ICO if individuals have data protection compliance concerns?
- Is a system of regular compliance reviews in place, including compliance with the provisions of the ICO Code of Practice, continued operational effectiveness and whether the system continues to meet its purposes and remains justified?
- Are the results of the review recorded, and are its conclusions acted upon?

The periodic review will also ensure all information is sufficiently protected to ensure that it does not fall into the wrong hands. This will include technical, organisational and physical security. For example:

- Sufficient safeguards are in place to protect wireless transmission systems from interception.
- The ability to make copies of information is restricted to appropriate staff.
- There are sufficient controls and safeguards in place if the system is connected to, or made available on a computer, e.g. an intranet.

- Where information is disclosed, it is safely delivered to the intended recipient.
- Staff are issued with guidance on security procedures and there are sanctions against staff who misuse surveillance system information.
- Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.
- The process for deleting data is effective and being adhered to.
- If there been any software updates (particularly security updates) published by the equipment's manufacturer that they have been applied to the system.

### **13. Complaints**

If you have a complaint about how your personal data has been handled by St Peter's Catholic Primary School, you should contact the Data Protection Officer in the first instance.

This policy does not outline the process for complaints and concerns which are directly related to the processing of personal data. Please see the school's Complaints policy if you have a complaint or concern which relates to another matter:

<https://www.stpeters.walsall.sch.uk/page/?title=Complaints+Procedure&pid=31>

Complaints or concerns which relate to data protection or information rights should be submitted in writing to [DPO@st-peters@wasall.sch.uk](mailto:DPO@st-peters@wasall.sch.uk)

The Data Protection Officer will conduct an internal review into your complaint and respond to you within one calendar month.

If you are unsatisfied with the response the School has provided, you have the right to contact the Information Commissioner's Office. You can do this online at:

<https://ico.org.uk/make-a-complaint/your-personal-information-concerns/>