St John the Baptist RC Primary School

CCTV Policy

September 2025 version

1. INTRODUCTION

This is the closed-circuit television (CCTV) Policy of St John the Baptist RC Primary School (the School). This CCTV Policy outlines how the School uses CCTV and processes the personal data obtained in accordance with data protection laws.

The School uses CCTV and the images/ recordings produced to:

- monitor entry to the school building;
- prevent or detect crime;
- keep its pupils, staff, and visitors in a safe and secure environment;
- prevent damage to the school property and its surroundings;

This list is not exhaustive and other purposes may be or become relevant.

This policy is intended to assist staff in complying with their own legal obligations when working with personal data.

2. DEFINITIONS

For the purposes of this policy, the following terms have the meanings provided below:

2.1. **CCTV**: means fixed and domed cameras designed to capture and record images of individuals and property.

2.2. **Data**: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

2.3. **Data subjects**: means all living individuals about whom the School hold personal information as a result of the operation of our CCTV (or other surveillance systems).

2.4. **Personal data**: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

2.5. **Data controllers**: are the School. The School is responsible for establishing practices and policies to ensure compliance with the law.

2.6. **Data users**: are authorised members of staff whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.

2.7. **Data processors**: are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

2.8. **Processing**: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

2.9. **Surveillance systems**: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes **CCTV** systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

2.10. **Data Protection Officer (DPO)**: The individual or organisation appointed by the School to monitor compliance with data protection laws, advise on data protection obligations, provide advice on Data Protection Impact Assessments (DPIAs), and act as the contact point for the Information Commissioner's Office (ICO).

3. ABOUT THIS POLICY

The School currently uses CCTV cameras to view and record individuals on and around its premises. This policy outlines why the School uses CCTV, how the School will use CCTV and how the School will process data recorded by CCTV cameras to ensure the School is compliant with data protection law and best practice. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

The School recognises that information held about individuals, including images recorded on CCTV, is subject to data protection legislation. Therefore, the School will seek guidance from its Data Protection Officer (DPO) to ensure that the processing of such footage is lawful before any processing takes place. The School is also committed to fulfilling all legal obligations and adhering to best practice guidance issued by the Information Commissioner's Office (**ICO**).

This policy covers all pupils, members of staff, volunteers, governors and visitors to the School. This policy has been agreed and implemented by the Governing Body.

This policy does not form part of the terms and conditions of any employment or other contract. The School may amend this policy at any time. The policy will be regularly reviewed by the School to ensure that it meets legal requirements and relevant guidance published by the ICO.

4. MONITORING

CCTV monitors the exterior of the building, and both the main entrance and secondary exits used by the School] [24 hours a day] and this data is continuously recorded**.**

Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on areas expected to be private, for example, toilets, changing cubicles, changing areas, etc.

Images are monitored by authorised members of staff in the course of their duties.

Staff using surveillance systems will be given appropriate training to ensure they understand and

observe the legal requirements related to the processing of relevant data.

5. HOW THE SCHOOL WILL OPERATE ANY CCTV

The School will ensure that signs are displayed at the entrance of the surveillance area to alert individuals that their image may be recorded. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety. The School will ensure that live feeds from cameras and recorded images are only available to approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters.

6. USE OF DATA GATHERED BY CCTV

In order to ensure that the rights of individuals recorded by the CCTV system are protected, the School will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

Given the large amount of data generated by surveillance systems, the School may store video footage using a cloud computing system. The School will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.

The School may engage data processors to process data on our behalf. The School will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

7. RETENTION AND ERASURE OF DATA GATHERED BY CCTV

Data recorded by the CCTV system will be stored on the School's database and server digitally using a cloud computing system. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. In all other cases, recorded images will be kept for no longer than 30 days. The School will maintain a comprehensive log of when data is deleted in accordance with its Retention Policy. At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

8. USE OF ADDITIONAL SURVEILLANCE SYSTEMS

Prior to introducing any new surveillance system, including placing a new CCTV camera in any area of the School, the School will carefully consider if they are appropriate by carrying out a data

protection impact assessment (**DPIA**).

A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

Any DPIA will consider the nature of the problem that the School is seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, the School will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

9. COVERT MONITORING

The School will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration the School will act in conjunction with the Police and the Local Authority.

In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with Judicial authorisation obtained by the Police or the Local Authority on behalf of the School. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision. Only limited numbers of people will be involved in any covert monitoring.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

10. ONGOING REVIEW OF CCTV USE

The School will ensure that the ongoing use of existing CCTV cameras in and around the School is reviewed at least every 12 months to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

11. REQUESTS FOR DISCLOSURE

Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

In other appropriate circumstances, the School may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

The School will maintain a record of all disclosures of CCTV footage.

Before providing CCTV footage in response to any request, the School will ensure that it is appropriate to do so and in accordance with the data protection legislation.

No images from CCTV will ever be posted online or disclosed to the media.

12. SUBJECT ACCESS REQUESTS (SAR)

Data subjects may make a request for disclosure of their personal information and this may include CCTV images (**subject access request**). A subject access request is subject to the statutory conditions in place and can be made verbally or in writing. It is recommended to make your request in writing, to assist individuals in retaining an audit trail.

In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

The School reserves the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where the School consider it necessary to do so.

The School may also refuse to disclose footage where an exemption applies under data protection legislation.

13. COMPLAINTS

Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

14. REQUESTS TO PREVENT PROCESSING

The School recognises that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the UK General Data Protection Regulation). For further information regarding this, please contact Kathleen McKeating (Headteacher).