Information Governance Support Services by Stockport Council

IGSS/P/003

St. Paul's C of E Primary School

CCTV Policy

Approved by the Resources Committee: Autumn 2026

Review Date: Autumn 2027

Contents

1. Introduction....3
2. Objectives of CCTV....3
3. Lawful Basis for Processing....3
4. Identification of CCTV cameras....4
5. Security and supervision of CCTV Systems....4
6. Storing digital images....5
7. Retention and erasure....5
8. Access to CCTV images....5
9. Breach Reporting....6
10. Installation of new CCTV systems....6
11. Complaints and queries....7
Document Control....8

1. Introduction

St. Paul's C of E Primary School operates a Closed-Circuit Television (CCTV) system to support the safety, security and wellbeing of pupils, staff, visitors and school property. CCTV is used to help prevent and detect crime, investigate incidents, protect the school site, and maintain a safe and secure environment.

The school's CCTV system consists of 2 fixed cameras located at appropriate areas across the school site. The school does not record audio through the CCTV system.

The school is the Data Controller for personal data captured by the CCTV system and is responsible for ensuring that CCTV is operated in accordance with UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). CCTV footage will only be collected and used where it is necessary, proportionate and for legitimate purposes set out within this policy.

2. Objectives of CCTV

The school uses CCTV for the following purposes:

- ensuring a safe environment for pupils, staff and visitors.
- deterring criminal acts against persons and property.
- assisting the police in identifying persons who have committed an offence.
- allowing for the prevention, investigation and detection of crime.
- monitoring the security of the site.
- allowing for the apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
- Ensuring damage to the automatic car park gate can be traced to the vehicle responsible.

CCTV will not be used for routine staff performance management, employee monitoring, pupil behavioural monitoring, or covert surveillance unless authorised and lawful under applicable legislation.

3. Lawful Basis for Processing

The school processes personal data obtained through CCTV under Article 6(1)(e) UK GDPR (Public Task) where it is necessary to carry out its functions as a school and to maintain a safe and secure environment. In some circumstances processing may also be necessary for the purposes of the school's legitimate interests in protecting pupils, staff, visitors and property. Further information about how the school processes personal data

through CCTV, including individuals' rights, can be found within the school's privacy notice on the school website.

4. Identification of CCTV cameras

Locations have been selected, both inside and out, that the school reasonably believes require monitoring to address the stated objectives.

In areas where CCTV is used the school will ensure that there are prominent signs in place to inform individuals they are entering a monitored area. These signs will contain:

- Details of the Data Controller operating the CCTV
- Contact details for further information regarding the system

5. Security and supervision of CCTV Systems

The school will implement appropriate technical and organisational measures to protect CCTV systems and the personal data they contain from unauthorised access, alteration, disclosure, loss or destruction.

Images from the CCTV system are only accessible to named individuals who are authorised to monitor CCTV for the stated objectives.

This includes the following positions:

- Headteacher
- School Business Manager
- School Office Manager
- Site Supervisor

Staff authorised to access CCTV footage will receive appropriate information governance and data protection training. The school will regularly review access permissions and security measures to ensure the continued confidentiality, integrity and availability of CCTV footage.

Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons. An audit trail of all access to, viewing of, extraction of, and disclosure of CCTV footage will be maintained.

Where CCTV systems are provided or supported by third-party suppliers, the school will ensure appropriate contractual arrangements are in place, including Data Processing Agreements where required.

6. Storing digital images

Recorded images will be stored in a way that ensures the integrity of the image and in a way that allows specific times and dates to be identified. Access to live images is restricted to the CCTV operator, unless the monitor displays a scene which is in plain sight from the monitored location.

Recorded images can only be viewed in a restricted area by approved staff. The recorded images are viewed only when there is suspected criminal activity and not for routine monitoring of pupils, staff or visitors.

The school reserves the right to use images captured on CCTV where there is activity that the school cannot be expected to ignore such as criminal activity, potential gross misconduct, or behaviour which puts others at risk. If a CCTV camera has recorded a specific incident under investigation, recordings may be used in both student and staff investigatory and potentially disciplinary proceedings to provide evidence as appropriate.

Images retained for evidential purposes will be retained in a locked area accessible by the system administrator only. Where images are retained, the system administrator will ensure the reason for its retention is recorded, where it is kept, any use made of the images and finally when it is destroyed.

7. Retention and erasure

Images captured by CCTV/Surveillance will not be kept for longer than is necessary. Images are stored on a 4GB hard drive which holds approximately 1 month of images. However, on occasions there may be a need to keep images for longer, for example where a crime is being investigated.

There is no specific minimum or maximum periods which apply to CCTV recorded images. The school ensures that images are not retained for longer than is necessary. Once the retention period has expired, the images are removed or erased.

8. Access to CCTV images

Requests for disclosure

CCTV footage will only be disclosed where there is a lawful basis to do so and where disclosure is necessary and proportionate. Requests may be considered from law enforcement agencies for the prevention, detection or prosecution of crime, from courts

or legal representatives in connection with legal proceedings, from insurers investigating incidents or claims, and from other organisations involved in safeguarding or regulatory functions where there is an appropriate legal gateway. All requests will be assessed on a case-by-case basis to ensure compliance with data protection legislation and the rights and freedoms of individuals.

Data will not normally be released unless satisfactory evidence has been provided demonstrating a lawful entitlement to access the footage.

Subject access requests

Under the UK GDPR and the DPA, individuals have the right to request access to personal data held about them, including CCTV footage where they can be identified. Further information about these rights can be found in the school's Data Subjects' Rights Guidance which can be found on the school's website. Requests may be made verbally or in writing, and the school may request proof of identity before processing the request. The school will normally respond within one calendar month.

To assist in locating relevant footage, requests should include, where possible, the date, time and location of the recording. Where CCTV footage contains images of other individuals, the school will consider the rights and freedoms of those individuals before any disclosure is made and may redact, obscure or withhold footage where required by data protection legislation.

The school will maintain a record of all disclosures of CCTV footage and the reasons for those disclosures. Requests relating to CCTV footage should be submitted to admin@st-pauls.stockport.sch.uk.

9. Breach Reporting

Any loss, unauthorised disclosure, misuse, or compromise of CCTV footage will be managed in accordance with the school's Personal Data Breach Policy.

10. Installation of new CCTV systems

CCTV has the potential to be privacy intrusive. The school will perform a Data Protection Impact Assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and addresses one of the stated objectives.

11. Complaints and queries

Any complaints, concerns or queries regarding the operation of the school's CCTV system, the use of CCTV footage, or the handling of personal data obtained through CCTV should be raised with the school in the first instance. Complaints will be investigated and responded to in accordance with the school's data protection complaints procedure.

Individuals who remain dissatisfied may contact the school's Data Protection Officer at igschoolsupport@stockport.gov.uk or lodge a complaint with the Information Commissioner's Office (ICO)

Document Control

Title	CCTV Policy
Document Owner	Information Governance – Stockport Metropolitan Borough Council
Document Status	For School Approval
Links with other policies, procedures, or guidance	CCTV and call recording privacy notice Personal data breach policy
Target Audience	School workforce, School governors
Distribution	Website, hard copy
File Classification	Public
Current Version	3.0

Revision and Approval

Reviewed by	SMBC IG Team
Issue Date	01/09/2026
Approved by (school)	TBC
Approval date	TBC
Next review date	01/09/2028
Any changes made	Complete review – Introduction changed. s3 – lawful basis for processing – **new** s5 - supervision includes security s9 - Breach reporting – **new** s8 - request disclosure changed s11 - complaints amended

Change History

Version	Author	Issue Date	Review date	Changes made?
V1	IG Team	28.10.2022	01/09/2024	New Policy
V2	IG Team	16/09/2024	01/09/2026	Minor amendments