# CCTV Policy

# St Agnes C of E Primary School

| | |
|---|---|
| **Approved by:** | Sue Gittins |
| **Last reviewed on:** | September 2026 |
| **Next review due by:** | September 2027 |

# CCTV Policy

## Our Christian Vision

*'Learning together in God's Love'*

### Our Christian Vision

St Agnes is an inclusive Christian family, we want our children to:

- Learn together with respect, patience and kindness
- **Treat each other as they would like to be treated (Matthew 7v12)**
- Flourish in education and friendships
- **Live life in all its fullness (John 10v10)**
- Be proud of themselves and others
- Ensure everyone is treated equally

Through the range of experiences we offer to all our pupils we encourage an understanding of the meaning and importance of faith and promote all the Christian Values. We particularly focus on Responsibility, Creativity, Forgiveness, Perseverance, Hope, Thankfulness and Friendship. These Christian values form the basis of our vision and are embedded throughout our school life and underpin all our teaching.

St Agnes is a small school that supports our community by providing an education of the highest quality within the context of Christian belief and practice. We work closely with our families to ensure they are fully supported and cared for.
We expect everyone at St Agnes C of E Voluntary Aided Primary School to follow 'The Great

Expectations' –

Be Safe
Be in the right place at the right time
Do your best
Handle your emotions
Use appropriate language
Cooperate
Respect everyone and everything

### 1. Introduction

The purpose of this policy is to regulate the management, operation and use of the school's closed-circuit television (CCTV) system, including its audio-recording capability, in a way that supports safeguarding and safety while respecting the privacy rights of pupils, staff and visitors.

St Agnes C of E Primary School operates one fixed camera in the Quiet Room. The Quiet Room is a designated reflection and de-escalation space where a child may go, with appropriate adult support, to calm and regulate. It is not a general circulation route or through-route within the school.

### 2. Purpose

The specific purposes of the CCTV system are to:

- support the safeguarding, welfare and physical safety of children and staff using the Quiet Room;

- provide an objective record of significant incidents where a child becomes distressed or dysregulated, including circumstances in which restrictive physical intervention or restraint may be required;
- assist the school to establish an accurate factual account following an injury, allegation, complaint, safeguarding concern or other serious safety incident;
- support appropriate review, learning and safeguarding action following such incidents; and
- provide relevant evidence to authorised external bodies where disclosure is lawful and necessary.

The system is not installed for general surveillance of pupils or staff, routine staff performance management, or general monitoring of movement around the school. CCTV does not replace appropriate staff supervision, safeguarding procedures, behaviour records or records of restrictive physical intervention.

**3. The System and Location**

The CCTV system is owned and operated by St Agnes C of E Primary School and comprises one fixed camera located in the Quiet Room, situated off the main hall near the large playground door.

Key features of the system are:

- the camera records video and audio;
- the camera is fixed to the Quiet Room and is not used to follow or target individuals elsewhere in school;
- recordings are held within the school's UniFi Protect system on secure on-site recording equipment;
- access is restricted to specifically authorised personnel using authorised accounts and designated, appropriately secured devices; and
- the field of view must remain limited to what is necessary for the stated safeguarding and safety purposes.

The current CCTV system does not use artificial intelligence, facial recognition, biometric identification, emotion recognition or automated behaviour analysis. Any proposal to introduce such functionality would require a separate assessment of necessity and proportionality, consultation with the DPO and DSL as appropriate, review or completion of a DPIA, and amendment of this policy before implementation.

The system is configured to record continuously so that the context before, during and immediately after an unexpected escalation can be available without requiring a member of staff to activate recording during an incident. Because continuous audio recording is particularly privacy-intrusive, the school must specifically justify and document its necessity and proportionality in the CCTV Data Protection Impact Assessment (DPIA) and review this at least annually.

Where the system is replaced or upgraded, the school will consider whether a less intrusive technical configuration, such as separately controlled or event-triggered audio, can meet the safeguarding purpose equally effectively.

**4. Data Protection, Lawful Use and Audio Recording**

The school will operate the system in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended, and current Information Commissioner's Office (ICO) guidance on video surveillance and monitoring workers.

The school will maintain the appropriate ICO data protection registration/fee arrangements that apply to it as a data controller. The school's lawful basis for the CCTV processing, together

with the purposes, retention period, access arrangements and any data sharing, will be documented in its records of processing, privacy information and DPIA. Consent is not relied upon as the general lawful basis for operating the system.

A current DPIA must be maintained for this system. The DPIA must specifically consider:

- the fact that the system records children, including children who may be distressed, dysregulated or vulnerable;
- the impact of recording staff in a workplace setting;
- the additional intrusion created by recording audio as well as video;
- why the safeguarding and safety purpose cannot be achieved as effectively through less intrusive means alone;
- the necessity of continuous rather than manually triggered recording;
- the camera field of view, access controls, retention period and security arrangements; and
- the wording and location of signs and privacy information.

The school's identified reason for retaining audio capability is that, in a de-escalation or physical-intervention incident, what is said can be important to understanding the context, including instructions, reassurance, warnings, distress, attempts to de-escalate and the sequence of events. Audio must not be used for general listening-in or routine monitoring of conversations.

If the annual review or DPIA no longer demonstrates an evidenced, necessary and proportionate need for audio recording, the audio function must be disabled.

**5. Transparency and Signage**

The CCTV system is overt. Pupils, staff, parents/carers and visitors must be given clear information about its existence and purpose. Signage at or immediately outside the Quiet Room must make clear that both video and audio are recorded, identify the school as the data controller and explain how further privacy information can be obtained.

The school's privacy information will explain, in clear and age-appropriate terms where relevant, why the Quiet Room is recorded, how long recordings are normally kept, who may access them, circumstances in which they may be shared and how individuals can exercise their data protection rights.

Staff will be informed about the nature and extent of the monitoring and the school will consult appropriately with staff when the DPIA or monitoring arrangements are materially changed.

**6. Operation and Permitted Access**

The Headteacher is responsible for the overall operation of the system and may delegate day-to-day administration to a named senior member of staff. Technical support may be provided by authorised IT personnel only to the extent necessary to maintain the system.

Recorded footage, live view and audio may only be accessed where there is a specific, legitimate reason connected to this policy. Examples include:

- responding to or reviewing an immediate safeguarding or health and safety concern;
- reviewing a significant incident in the Quiet Room, including a restrictive physical intervention or restraint;
- investigating an injury, allegation, complaint or serious behaviour/safety incident;
- preserving evidence relevant to safeguarding, disciplinary, legal or insurance processes;
- responding to a valid data protection rights request or lawful request from an external authority; and

- undertaking proportionate technical checks to confirm that the system is operating correctly.

Live viewing must not be used as a substitute for appropriate supervision of a child in the Quiet Room or for routine observation of staff. Any live access must be necessary for an immediate safeguarding, safety or technical purpose.

All non-routine access to recordings should be logged with the date, person accessing the footage, reason for access and any action taken or disclosure made.

**7. Safeguarding and Restrictive Physical Intervention**

Where a child requires support in the Quiet Room, staff must continue to follow the school's safeguarding, behaviour, positive handling/restrictive physical intervention and recording procedures. The existence of CCTV does not alter the legal and professional requirements governing the use of physical intervention.

Where restrictive physical intervention, an injury, an allegation against an adult or another significant safeguarding incident occurs in the Quiet Room, the Headteacher or DSL should consider promptly whether relevant CCTV footage should be preserved before routine overwrite. Access must be limited to those who need to review the incident for a legitimate safeguarding, employment, legal or regulatory purpose.

Footage may assist in establishing facts, but it must be considered alongside other relevant evidence, including the child's account where appropriate, staff accounts, incident records, medical information and safeguarding records. CCTV footage must not be treated as the sole determinant of whether an intervention was necessary, reasonable or proportionate.

**8. Security, Devices and System Control**

The UniFi Protect system and recording equipment must be secured against unauthorised access. Access credentials must be individual where the system allows, protected appropriately and not shared except where an authorised technical process requires it.

CCTV footage must not be routinely accessed, downloaded, screen-recorded or stored on personal phones, tablets, laptops, smartwatches, personal cloud storage or other bring-your-own devices. Remote or mobile access may only take place using a school-authorised account and a school-approved, appropriately secured device. No copy of footage may be retained locally on a personal device.

Visitors or contractors requiring technical access must be authorised, appropriately supervised and limited to the minimum access necessary. Technical access must not include viewing recordings unless this is necessary for the specific maintenance task.

System checks and maintenance will be recorded. The Headteacher or nominee will ensure that the camera, audio function, storage, date/time settings, access controls and overwrite process are checked periodically.

**9. Storage, Retention and Preservation**

Routine recordings are retained within the UniFi Protect system for a maximum of 30 days and are then automatically overwritten. The 30-day period is a school retention decision and must be reviewed through the DPIA to ensure it remains no longer than necessary for the safeguarding and safety purposes of the system.

Relevant footage may be preserved beyond 30 days where it is required for a specific purpose, including a safeguarding investigation, restrictive physical intervention review, complaint, allegation, accident or injury investigation, insurance matter, legal proceedings, subject access request or police investigation.

Preserved footage must be securely restricted and deleted as soon as it is no longer required for the purpose for which it was retained.

Where footage must be exported, it must be transferred to an approved encrypted school storage location or approved encrypted removable media. Personal USB drives or unencrypted removable media must not be used. Each export must be logged and, where relevant, a chain-of-custody record maintained.

**10. Disclosure to Police and Other Third Parties**

The school may disclose CCTV footage to the police, local authority, insurers, legal advisers, safeguarding partners or other third parties where disclosure is lawful, necessary and proportionate. The school will consider each request on its facts and will not disclose footage merely because it has been requested.

Requests and disclosures must be recorded, including the identity of the requester, purpose of the request, footage disclosed, date of disclosure and the school's justification or legal basis. Where appropriate, the DPO should be consulted before disclosure.

Footage will not be released to the media or published publicly unless there is a clear lawful basis and specific authorisation following appropriate legal and data protection advice.

**11. Subject Access and Individual Rights**

Individuals have data protection rights in relation to personal data captured by the CCTV system. A subject access request (SAR) may be made verbally or in writing. Requests should be passed promptly to the Headteacher/DPO so that relevant footage can be identified and, where necessary, protected from routine deletion.

The school will normally respond to a SAR without undue delay and within one month, subject to any lawful extension, pause or exemption that applies. The school may request proportionate information needed to identify the requester and locate the footage.

Where a requester is entitled to a copy of CCTV information, the school will provide the relevant personal data in an appropriate form. It will not operate a blanket rule that only still images are supplied. Where necessary, the school will redact or obscure third-party images and/or audio, or use another lawful method to protect the rights of others.

Requests made by a parent or carer on behalf of a child will be considered in accordance with the child's data protection rights, age and understanding, parental responsibility, safeguarding considerations and any applicable exemptions. The DPO should be consulted where the position is unclear.

**12. Covert Surveillance**

This policy authorises overt CCTV only. The Quiet Room camera must not be converted or used for covert or targeted surveillance under this policy. Any proposal for covert monitoring would require a separate, documented assessment and appropriate legal and data protection advice before any action is taken. It must not be authorised simply by a routine Headteacher decision under this CCTV policy.

**13. Breaches, Complaints and Incidents**

Any suspected unauthorised access, disclosure, loss, copying or misuse of CCTV footage must be reported immediately to the Headteacher and the school's Data Protection Officer and managed under the school's data protection breach procedures. Where required, the DPO will consider notification to the ICO and affected individuals.

Complaints about the operation of CCTV should be made to the Headteacher and will be considered under the school's complaints and data protection procedures. Individuals may

also raise data protection concerns with the school's DPO and have the right to complain to the ICO.

Serious misuse by staff may be dealt with under the school's disciplinary procedures. Safeguarding concerns arising from CCTV use or footage must be referred to the DSL and managed under the school's safeguarding procedures.

**14. Monitoring and Annual Review**

The Headteacher and DPO, with appropriate governing body oversight, will review the CCTV arrangements at least annually and whenever there is a material change to the system, room use, safeguarding purpose or applicable guidance.

The review will include:

- whether the camera remains necessary for the Quiet Room;
- whether audio recording remains specifically justified, necessary and proportionate;
- whether continuous recording remains necessary;
- the DPIA, lawful basis and privacy information;
- camera field of view and signage;
- access logs, security controls and any personal-device access;
- the 30-day retention period and any preserved footage;
- any complaints, safeguarding incidents, breaches or disclosures; and
- whether a less intrusive technical solution could now meet the same safeguarding purpose.

**15. Protecting Personal Data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR).

- The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.

- All data will be handled in accordance with the school's Data Protection Policy.

| Data Audit For This Policy | | | | | |
|---|---|---|---|---|---|
| **What ?** | **Probable Content** | **Why ?** | **Who ?** | **Where ?** | **When ?** |
| CCTV video and audio recordings | Images, voices, actions, date/time and contextual information relating to use of the Quiet Room | Safeguarding and safety; reviewing significant incidents, injuries, allegations or restrictive physical intervention | Pupils, staff and occasional authorised visitors | UniFi Protect system on secure on-site recording equipment | Normally retained for a maximum of 30 days, then automatically overwritten unless required for a specific documented purpose |

| | | | | | |
|---|---|---|---|---|---|
| CCTV access and export records | Date/time of access, person accessing footage, reason for access, details of any export or disclosure | Accountability, security and demonstrating appropriate use of CCTV information | Authorised staff and, where applicable, authorised external recipients | Secure school records/systems | Retained in accordance with the school's data retention arrangements |

- As such, our assessment is that this policy :

| Has Few / No Data Compliance Requirements | Has A Moderate Level of Data Compliance Requirements | Has a High Level Of Data Compliance Requirements |
|---|---|---|
| | | ✓ |

## Appendix 1A: Camera and Purpose Log

| | |
|---|---|
| **Camera** | 1 - fixed CCTV camera |
| **Location** | Quiet Room - designated reflection/de-escalation space; not a general school through-route |
| **Recording** | Video and audio |

| | |
|---|---|
| **Primary purpose** | Safeguarding and safety of pupils and staff; factual review of significant incidents, including restrictive physical intervention where necessary |
| **System/access** | UniFi Protect; secure on-site recording; authorised personnel and approved devices only |
| **Routine retention** | 30 days unless preserved for a specific documented purpose |

### Appendix 1B: Transparency and Signage Requirements

- A clear sign at or immediately outside the Quiet Room stating that CCTV video and audio recording is in operation.
- The sign should identify St Agnes C of E Primary School as the data controller and give a contact point or route to the school's privacy information.
- The school's staff and pupil/parent privacy information should explain the specific Quiet Room safeguarding purpose, audio recording, retention and rights.

### Appendix 2: CCTV Data Audit

| | |
|---|---|
| **Data** | CCTV video, audio, date/time metadata, access and export logs |
| **Likely content** | Images, voices, actions and contextual information relating to incidents in the Quiet Room |
| **Purpose** | Safeguarding, health and safety, incident review, legal/data protection rights and lawful external disclosure |
| **Who is recorded** | Pupils, staff and occasional authorised visitors to the room |
| **Storage/access** | UniFi Protect/on-site recorder; preserved copies only on approved secure school storage; authorised access only |
| **Retention** | Normally 30 days; longer only where required for a specific documented purpose |

**Data compliance assessment: HIGH - the system processes video and audio involving children and staff and therefore requires strong access controls, transparency, documented necessity/proportionality and a current DPIA.**