ROSSETT ACRE PRIMARY SCHOOL

CCTV Policy

Name of School: Rossett Acre Primary School
Member of staff responsible: Kate Woodcock
Date of Policy: January 2023

Date of next review: 8th January 2024, 29th January 2025, January 2026

Reviewed September 2026 - January 2027

The school recognises that CCTV systems can be privacy intrusive.

For this reason, the school has carried out a data protection impact assessment to evaluate whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below.

The school is the data controller for CCTV images processed for school purposes. The school will work with the Data Protection Officer to ensure that the system remains lawful, necessary, proportionate and appropriately documented.

The result of the data protection impact assessment has informed the school's use of CCTV and the contents of this policy.

Objectives

Review of this policy shall be repeated regularly and whenever new equipment is introduced, a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

The purpose of the CCTV system is to assist the school in reaching the following objectives:

(a) To protect pupils, staff and visitors against harm to their person and/or property;

(b) To increase a sense of personal safety and reduce the fear of crime;

(c) To protect the school buildings and assets;

(d) To support the police in preventing and detecting crime;

(e) To assist in identifying, apprehending and prosecuting offenders;

(f) To assist in establishing the cause of accidents and other adverse incidents and help prevent recurrence; and

(g) To assist in managing the school.

Purpose of This Policy

The purpose of this policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the school. The CCTV system used by the school consists of 13 cameras.

CCTV cameras are not installed in any indoor areas.

Statement of Intent

CCTV cameras are installed in such a way that they are not hidden from view. Clear and visible signs are displayed where relevant so that staff, pupils, parents, carers, visitors and members of the public are made aware that they are entering an area covered by CCTV. Signs will identify the school as responsible for the system and provide appropriate contact details.

The CCTV system will comply with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and will have regard to current Information Commissioner's Office (ICO) guidance on video surveillance and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012.

The school will treat the system, all information, documents and recordings, including images of identifiable pupils, staff, parents, carers, visitors and members of the public, as personal data where individuals can be identified. Such information will be processed lawfully, fairly and transparently and only for the purposes set out in this policy.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system 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 will be clearly visible on the school site and will support transparency by making clear who is responsible for the equipment, the general purpose of the recording and how individuals can raise questions or exercise their information rights.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Routine CCTV footage is automatically overwritten by the system after 28 days unless it has been extracted and retained for a specific, documented reason.

Recorded images may be retained for longer than the routine 28-day period only where this is necessary for a specific purpose, such as an accident, safeguarding concern, complaint, behaviour incident, insurance or legal matter, police request or ongoing investigation. Any extended retention will be documented, kept under review and deleted securely when no longer required.

System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be administered and managed by Kirsty Macnair, School Business Manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager, the system will be managed by Donna Misseldine, Senior Administrator.

The system and the data collected will only be available to the System Manager, their nominated replacement and appropriate members of the senior leadership team as determined by the Headteacher. Access will be limited to those who require it for the purposes set out in this policy.

The CCTV system is designed to be in operation 24 hours each day, every day of the year, though the school does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned above requests access to the CCTV data or system, the System Manager must satisfy themselves of the identity of the requester and the legitimacy and necessity of the request. Where any doubt exists, access will be refused or advice will be sought from the school's Data Protection Officer.

Details of all access to the CCTV system, including visits by authorised visitors, will be recorded in a system log. The log will include the date and time of access, the person accessing the system, the images viewed or copied, the reason for access and any disclosure made.

Downloading Captured Data on to Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures: -

(a) Each downloaded media must be identified by a unique mark.

(b) Before use, each downloaded media must be cleaned of any previous recording.

(c) The System Manager will register the date and time of downloaded media insertion, including its reference.

(d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.

(e) If downloaded media is archived, the reference must be noted.

(f) If downloaded media is put onto a device, the device will be encrypted and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the System Manager, their nominated replacement, the Headteacher and other authorised senior leaders. However, where one of these people may later be called as a witness to an offence and where the data content may be used as evidence, it shall be preferable, where possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the school and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the school's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's Data Protection Officer.

Complaints About the Use of CCTV

Any complaints in relation to the school's CCTV system should be addressed to the Headteacher.

Requests for Access by the Data Subject

Individuals have the right to request access to CCTV images of themselves where they can be identified. Requests should be made to the Headteacher or the school's Data Protection Officer. The school will respond within the statutory timescale, normally one calendar month, and will take reasonable steps to verify identity and protect the rights and freedoms of others who may appear in the footage, including pupils. Where necessary, images may be redacted or access may be refused in line with data protection legislation.

Public Information

Copies of this policy will be available to the public from the school office and may also be made available through the school website or privacy information where appropriate.