Rye Primary Policy

Policy Title:	Surveillance and CCTV
Leadership Responsibility:	Academies Business Manager
Review Body:	Head Teacher
Date:	November 2026
Review:	November 2027

Statement of Intent

At Rye Primary we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with the UK General Data Protection Regulations (GDPR).
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing.
- Taking action to prevent a crime.
- Using images of individuals that could affect their privacy.

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors
- Deter criminal acts against persons and property
- Assist the police in identifying persons who have committed an offence

Legal Framework

This policy has due regard to legislation including, but not limited to, the following:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (GDPR)

- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004
- Equality Act 2010

This policy operates in conjunction with the following statutory and non-statutory guidance:

- Home Office 'The Surveillance Camera Code of Practice'
- ICO 'A guide to the data protection principles'
- ICO 'CCTV and video surveillance'
- DfE 'Data protection in schools'
- Biometrics and Surveillance Camera Commissioner 'Surveillance Camera Code of Practice'

This policy operates in conjunction with the following policies:

- Aquinas Data Protection Policy
- Aquinas Online Safety Policy
- School Security Policy

Definitions

For the purpose of this policy the following definitions are given for the below terms:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g., real-time recordings and live streams. For the purpose of this policy only video footage will be applicable.
- **Overt surveillance** – Surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000.
- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

Rye Primary does not condone the use of covert surveillance when monitoring staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

Roles and Responsibilities

The role of the **Data Protection Officer** (DPO) will include:

- Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.

- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Considering the appropriate lawful basis to use to legitimise CCTV use.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Advising on whether the use of CCTV is appropriate and proportionate for the school's circumstances.
- Advising on where to place security cameras within the school.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the school, e.g. the Board of Trustees.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's data protection impact assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the Board of Trustees.

Aquinas, as the corporate body, is the data controller. The Head Teacher, therefore, has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The DPO deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

The role of the Head Teacher includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

Purpose, justification and transparency

The school will only use surveillance cameras for the safety and security of the school, and its staff, pupils and visitors. This may include, but is not limited to:

- Assisting in emergency situations.
- Managing lockdowns.
- Supporting the application of internal policies.
- Supporting the safeguarding of pupils.
- Providing a sense of security for pupils and staff.

The school will consider which lawful basis is most appropriate to use. This will be either public task of legitimate interests.

When using legitimate interests as its lawful basis, the school will complete a legitimate interests assessment.

Consent will not be appropriate as the lawful basis for the school's use of CCTV due to the unlikelihood of being able to obtain consent from everyone who may be captured on CCTV, because it is difficult for people to opt out.

In deciding whether CCTV is appropriate, the school will consider why it is necessary and appropriate.

The school will only conduct surveillance as a deterrent for violent behaviour and damage to the school environment. Under no circumstances will the surveillance and the CCTV cameras be present in classrooms, changing facilities, toilet cubicles.

If the surveillance and CCTV systems fulfil their purpose and are no longer required, or it is deemed such systems cannot be justified, the school will deactivate them and explore less intrusive alternatives.

In its use of surveillance and CCTV, the school will be open and honest towards the school community.

Clearly visible signs will also be in place to inform people that CCTV is in use.

Data Protection

Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a DPIA or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interest's assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
    - Further processing for archiving data in the public interest
    - Scientific or historical research
    - Statistical purposes

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The use of surveillance cameras and CCTV, will be critically analysed using a DPIA, in consultation with the DPO.

A DPIA will be carried out prior to the installation of any surveillance or CCTV system. A DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

- If the DPIA reveals any potential security risks or other data protection issues, the school will ensure it has provisions in place to overcome these issues.

- Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

- While data protection laws do not prescribe any specific minimum or maximum retention periods for CCTV footage, the school will not hold on to footage longer than is necessary. CCTV footage will ordinarily be deleted after **31 days**. Footage may be held for longer in exceptional circumstances, e.g., if it is required to assist a criminal investigation or because of a subject access request.

- The school will not use CCTV with live-facial recognition technology as this is unlikely to be justifiable. If the system chosen by the school does contain this feature, it will be switched off by default to ensure biometric data is not unnecessarily processed.

- CCTV will not be used to record conversations or otherwise act as an overly intrusive means of security. Any system that has the capability to record audio will have this feature switched off.

Protocols

The surveillance system will be registered with the ICO in line with data protection legislation.

The surveillance system is a closed digital system which does not record audio.

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. Warning signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

The surveillance system has been designed for maximum effectiveness and efficiency; however the school cannot guarantee that every incident will be detected or covered and 'blind-spots' may exist.

The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

Security

In exceptional cases where large amounts of information need to be collected and retained, the school will consider using cloud storage. This will be secure and only accessible to authorised individuals.

Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

The school's authorised CCTV system operators are:

- Ms F. Brassleay, Head Teacher
- Mrs R. Watkins – Deputy Headteacher
- Premises Team – for security and site maintenance
- Schools ICT Team – for maintenance

The main control facility is kept secure and locked when not in use.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

Surveillance and CCTV systems will be tested for security flaws termly to ensure that they are being properly maintained at all times.

The DPO and Head Teacher will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders.

Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

The ability to produce copies of information will be limited to the appropriate staff.

Any unnecessary footage captured will be securely deleted from the school system.

Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

Visual display monitors are located in the Deputy Headteacher's office, English Block server room and Premises office.

Code of Practice

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All surveillance footage will be kept for **31 days** for security purposes; the Head Teacher and DPO are responsible for keeping the records secure and allowing access.

The school surveillance and CCTV system will be in place for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available on the school website.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point which enables people to request information and submit complaints via the DPO.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up to date.

Access

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

All disks and hard drives containing images belong to, and remain the property of, the school.

Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing. SARs will be handled in accordance with the Subject Access Request (SAR) Policy.

Individuals maintain the right to have personal data erased if:

- The data is no longer necessary for the original purpose it was collected for.
- They are relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.
- The data has been processed unlawfully.
- There is a specific legal obligation.

There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- Where the processing is needed for the performance of a task in the public interest or an official authority.

- Certain research activities.
- Compliance with a specific legal obligation.

As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by the school or they object to way it was processed.

Data can be restricted by either:

- Moving the data to another processing system.
- Making the data unavailable to users.
- Temporarily removing published data from a website.

The school will verify the identity of the person making the request before any information is supplied. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

The school will ensure that all recorded CCTV footage is stored securely to maintain its confidentiality, integrity and availability.

Access to CCTV footage will be strictly controlled. Only authorised members of staff will be permitted to view, retrieve or manage CCTV recordings. This will ensure that the rights of any recorded persons are protected at all times.

The school will regularly review access permissions to ensure they remain appropriate, particularly where staff roles change or individuals leave the organisation.

The school will implement appropriate technical and organisational measures to prevent unauthorised access to CCTV data. Where possible, footage will be encrypted. Where encryption is not in place, the school will ensure that alternative safeguards are applied, including:

- Restricting access to designated staff only.
- Implementing appropriate security controls and safeguards.
- Ensuring CCTV equipment and control rooms are physically secure.
- Applying regular software updates and security patches.

The school will ensure that all staff with access to CCTV systems:

- Are appropriately trained in the use of the system.
- Understand their responsibilities in relation to data protection.

- Are familiar with relevant school policies on the handling of personal data.

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Requests for access or disclosure will be recorded and the headteacher will make the final decision as to whether recorded images may be released to persons other than the police. The school reserves the right to restrict viewing of video footage to an accompanied viewing on the school premises.

A copy of redacted static images will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Head Teacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

Use of automatic number-plate recognition (ANPR)

The school may consider the use of Automatic Number Plate Recognition (ANPR) systems within its car park. As these systems collect and process personal data in real time, their use will be carefully assessed to ensure it is necessary and proportionate.

ANPR systems will capture vehicle registration numbers, along with the date, time and location of entry or exit. This information will be treated as personal data, as it can be linked to identifiable individuals.

Prior to implementing any ANPR system, the school will complete a DPIA to assess risks and ensure compliance with data protection legislation. The school will ensure that only data necessary for the stated purpose is collected.

Clear and prominent signage will be displayed to inform individuals that ANPR is in use and to provide details on how to contact the school with any queries regarding the processing of their data.

Monitoring and review

This policy will be monitored and reviewed on an annual basis by the Deputy Headteacher and Head Teacher.

The Head Teacher will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.

The Head Teacher will communicate changes to this policy to all members of staff.

DATA PROTECTION

Rye Primary [The Academy] processes personal data in accordance with the data protection principles embodied in the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. The Academy complies with the requirements of the data protection legislation as detailed in the Trust Data Protection Policy.

All colleagues are aware of the principles of data protection and will not process personal data unless necessary. The Academy safeguards the personal data it collects through the operation of the Trust's data protection policy and processes and the IT policy. In addition, the Academy has taken steps to ensure that all its contracts that process data have the GDPR compliant provisions.