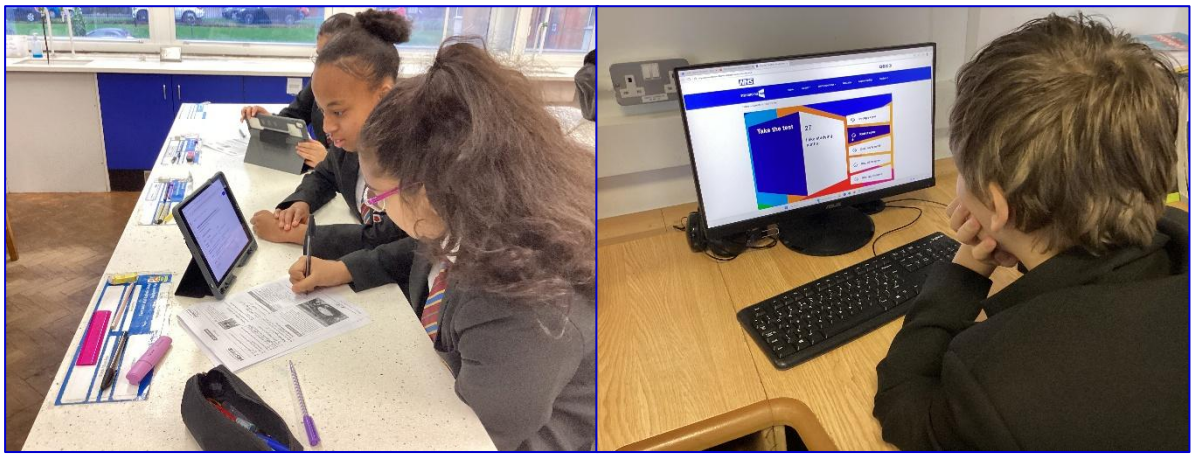

CCTV Policy

"The Lord watches over all who love him."
Psalm 145:20

Contents

Aims

Saint John Wall Catholic School currently uses CCTV cameras to view and record individuals on and around its premises. This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property and outlines how the School uses CCTV and processes the personal data obtained in accordance with data protection laws.

Saint John Wall Catholic School recognises that information held about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras in the School and on the School grounds is personal data and therefore subject to the legislation. The School is committed to complying with all our legal obligations and seek to comply with best practice suggestions from 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. Saint John Wall Catholic 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.

Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe and secure in the school environment
- Protect members of the school community from harm to themselves or to their property
- Prevent or detect criminality in the school
- Monitor entry to the school building
- Protect school assets, buildings and its surroundings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of behaviour, safeguarding, disciplinary or grievance proceedings
- To assist in the defense of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident or investigation occurring
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

Relevant Legislation and Guidance

This policy is based on:

Legislation

- UK General Data Protection Regulation Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000 The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 The School Standards and Framework Act 1998
- The Children Act 1989 The Children Act 2004 The Equality Act 2010

Guidance

- Surveillance Camera Code of Practice (2021)

Definitions

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

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

1.2. 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.

1.3. 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).

1.4. 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.

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

1.6. 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.

1.7. 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).

1.8. 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.

1.9. Surveillance systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals.

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.

Location of Cameras and Monitoring

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system

Cameras are currently located in:

Outside	**Indoors**
Main reception outside	Reception door
Main reception car park	Reception by monitors desk
RE corridor view outside	Stairs leading to changing rooms
Outside rooms 9 and 10	Hall entrance by car park
Year 10 and Year 11 playground	Door A/Heads of Years offices
Year 7 playground	Door C
Year 8 and Year 9 playground	Door B
Sink area outside	Science corridor
Canopy outside	Technology door inside by T6
Technology door entrance outside by T6	Door by SEND office
Top of Lane by school house	By room 3
Containers by canteen	Music room corridor
Staff car park by hall	Staffroom
Staff car park by gym	
Staff car park by reception entrance	
Changing room roof	

Signage is in place to warn members of the school community that they are under surveillance.

CCTV monitors the interior/exterior of the building, main corridors internally and both the main entrance/exit and pupil entrance/exits used by the School, 24 hours a day, 365 days a year.

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.

Surveillance systems will not be used to record sound.

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.

The system is registered with the Information Commissioner's Office.

Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

Roles & Responsibilities

The Governing Board

The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

The Headteacher

The headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

The Data Protection Officer

The data protection officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to

CCTV footage The System Manager

The system manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly

Operation of CCTV system

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.

Retention & Erasure of Data gathered by CCTV

In order to ensure that the rights of individuals recorded by the CCTV system are protected, Saint John Wall Catholic 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.

Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

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.

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.

Access to CCTV footage

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

Staff Access

The following members of staff have authorisation to access the CCTV footage:

- The Headteacher
- The Senior Leadership Team
- Pastoral Leaders
- The Data Protection Officer
- The System Manager
- Anyone with express permission of the headteacher

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

Subject access requests (SAR)

According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the request, the school will immediately issue a receipt and will then respond within 30 days during term time. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

School Leaders and Senior Administrators have received training to recognise SARs. When a SAR is received staff should inform the DPO in writing. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Files will be shared securely.

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

Records will be kept showing the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the headteacher and the DPO.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance

with UK GDPR. All disclosures will be recorded by the DPO.

Data Protection Impact Assessment (DPIA)

The school follows the principle of privacy by design. Privacy is considered during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in section 1).

When the CCTV system is replaced, developed or upgraded, or any new surveillance system is introduced, a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by HY Education.

Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be done annually and/or whenever cameras are moved, and/or new cameras are installed.

If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

Security

The system manager will be responsible for overseeing the security of the CCTV system and footage

The system will be checked for faults once a term

Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure

Footage will be stored securely and encrypted wherever possible

The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use

Proper cyber security measures will be put in place to protect the footage from cyber attacks

Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

Complaints

Complaints should be directed to the Headteacher or the DPO and should be made according to the school's complaints policy.

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 the School Business Manager.

Monitoring

The policy will be reviewed annually, along with the ongoing use of the CCTV system by the School Business Manager/DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

Links to Other Policies

- Cyber Security Policy
- Data Protection Policy – Pupils and Parents
- Online Safety Policy for staff & pupils
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding and Child Protection Policy

Ratified by Governors: 24/06/2026
Next Review Date: 24/06/2027
(This policy will remain in force beyond the review date if no updates are required)