CCTV Policy

Mission Statement

St John Rigby College is a Catholic College dedicated to the education and development of the whole person and supporting all students to realise their full potential. In becoming an outstanding learning organisation SJR will have a strong sense of purpose and a commitment to shared values within a Christian community. We will provide a unique and challenging environment where every individual is valued, talents are recognised and nurtured, achievements are celebrated and dedication is rewarded. To achieve this as a community we will:

- Welcome all students who are happy to be educated within a Christian environment
- Value the uniqueness and dignity of each individual
- Provide the highest standards of teaching and learning
- All show a commitment to our work and the Christian values of the College
- Provide equality of opportunity, with mutual respect and positive encouragement
- Build and further develop local, national and international partnerships

Core values in daily life at St John Rigby College are expressed as:

- Genuine concern for others
- Support for and challenge of one another
- High standards and expectations
- Consistency and perseverance
- Recognition of talents, progress and achievements.

Scope of Policy

The purpose of this policy is to regulate the management and use of CCTV at St John Rigby College. The policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The 'Surveillance Camera Code of Practice'
- ICO (2017) 'In the Picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2017) 'Overview of the General Data protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

This policy outlines how St John Rigby College complies with the 12 guiding principles given in the 'Surveillance Camera Code of Practice'.

1. **Aim of the CCTV System**
   Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need

   The College uses CCTV to help maintain an environment for students, staff and visitors, which supports their safety and welfare; to assist in the prevention of disorder or crime against persons and College property or assets and to assist in the identification and prosecution of persons having committed an offence.

2. **Individuals Privacy**

The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified

CCTV cameras are not used in any area of the College where there is a particularly high expectation of privacy, such as toilets or changing rooms.

The cameras do not focus on private homes, gardens or other areas of private property adjacent to the College.

The system does not make audio recordings.

3. **Information and Complaints**
There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints

All areas of the College where cameras are in use are identified with appropriate CCTV signage.

All staff and students are made aware of the CCTV system via their respective inductions and this policy is available to all staff, students and members of the public via the College web site, along with copies of any relevant management information, reviews, audits and statistical information on the number and nature of complaints received and how these have been resolved.

Complaints regarding the use of the CCTV system should be made in writing to the Principal.

The College will share information about the nature of complaints with the Surveillance Camera Commissioner to assist with the review of the operation of this policy.

4. **Responsibility and Accountability**
There must be clear responsibility and accountability for all surveillance camera system activities, including images and information collected, held and used

Governing Body: The Governing Body has the responsibility to ensure that there is a clear written policy statement that outlines how the College complies with CCTV regulations and delegate the management of the system to the Principal.

Principal: The Principal is responsible for the development and operation of the system via the delegation of roles, authority and duties for the use, management and maintenance of the CCTV system to the relevant staff and ensures that they are informed of these responsibilities and trained to carry them out. The Principal will provide annual reports to the Governing Body and investigate any reported breaches of the CCTV Policy by staff.

Vice Principal (Students): The Vice Principal (Students) is responsible for overseeing the work of the Student Liaison Officer in connection with the safety and welfare of students and to assist in the prevention of disorder or crime against persons and College property or assets. In the absence of the Vice Principal (Students), this responsibility is delegated to members of the Senior Leadership Team (SLT).

Data Protection Officer (DPO): The DPO is responsible for staying up to date with the Data Protection regulations (General Data Protection Regulation (May 2018)), auditing the correct usage of CCTV in line with this legislation and implementation of this policy.

Central Services Manager (CSM): The CSM is responsible for the day to day use of the CCTV system in line with this policy, the management, maintenance and repair of the CCTV system, staying up to date with relevant CCTV legislation, staff training arrangements and provision of reports to the SLT.

Finance Manager: The Finance Manager is responsible for negotiating the terms of contracts with the CCTV equipment supplier and other related security companies.

National Integrated Solutions Ltd: After normal College hours, the perimeter CCTV cameras are monitored external CCTV operators, who respond to motion sensor alarms and use the audio warning system to inform unauthorised intruders that they are being monitored via CCTV. In the event the intruder does not comply with the request to leave the site, Top Marks Security or the Police will be contacted as appropriate.

Top Marks Security: Top Marks Security provide an on-site security presence in response to calls made by Security One and are the appointed key holders for the College. In the event of a problem with the CCTV equipment, Top Marks Security are authorised to reset the CCTV system.

5. **Policy, Procedure and Communication**
Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them

The CCTV system is operated in line with this policy, which is shared with all staff and students via the Staff Information System. A copy of this policy is available on the College web site for members of the public.

A separate CCTV Hand Book outlines the specific procedures to be followed by the relevant staff.

6. **Storage of Data**
No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged

The system records 30 days of footage, after which the footage cannot be retrieved.

The College has the right to download images where there is suspicion that a crime has been committed. On occasion it may be necessary to retain downloaded images or footage for a longer period, for example when a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Any downloaded images or footage will be destroyed once they are no longer required for an active investigation.

7. **Access to Images and Information**
Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

The Principal has authorised the CSM to access CCTV footage to enable them to carry out their duties.

The CSM can authorise other relevant staff to view footage to assist in identifying staff, students or members of the public on a case by case basis.

Disclosure of images have to be made in writing and be approved by the Principal and the CSM.

Disclosure of images and information to law enforcement agencies have to be made in writing and be approved by the Principal and the CSM.

Subject Access requests have to be made in writing on the relevant form which can be obtained from the College on request. Subject Access requests will incur a £10 administration fee and will be actioned within 20 days.

Where images are disclosed, consideration will be given to whether images of other individuals should be obscured to prevent unwarranted identification.

CCTV footage will not be released to the media, or used for commercial purposes, or for the purpose of entertainment.

8. **Competency Standards**
Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

The CSM holds the Security Industry Authority (SIA) Level 2 Award for Working as a CCTV Operator (Public Space Surveillance) within the private security industry and is licenced accordingly.

9. **Security**
Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use

Logs are kept of access to the system by the CSM; giving the date, time and reason for access.

A review of retained footage can only be carried out if authorised by the Principal and the CSM.

Footage downloaded for evidence is recorded and controlled via an approved evidence system.

Logs and records relating to the CCTV system are kept in locked cabinets.

The CCTV system is regularly maintained.

10. **Review and Audit**
There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published

The CCTV system and policy are reviewed every two years to ensure it remains necessary, proportionate and effective in meeting its purpose.

The camera locations are reviewed every two years and alternative interventions are considered to determine if they provide less risk to individual privacy.

11. **Support of Public Safety and Law Enforcement**
When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value

The main purpose of the College's CCTV system is to help maintain an environment for students, staff and visitors, which supports their safety and welfare, however there may be instances where footage from the system can assist in crime prevention, detection and investigation.

To ensure the forensic integrity of recorded images and information evidence will be handled in line with the Police & Criminal Evidence Act (1984).

12. **Reference Database**
Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date

The College does not use the CCTV footage to record data that is compared against a reference database.

Relevant Legislation

Use of the CCTV system will have due regard to the following legislation:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation
- 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
- Data Protection Act (1998)
- Equality Act (2010)
- Disability Discrimination Act (1995)
- Employment Equality Act (2006)
- Human Rights Act (1953)
- Police & Criminal Evidence Act (1984)
- Race Relations Act (1976)
- Regulation of Investigatory Powers (2000)
- Sex Discrimination Act (1975)

Related Policies

- Data Protection Policy
- Freedom of Information Policy
- Information Systems Security Policy