SAINT GEORGE CATHOLIC COLLEGE

CCTV Policy

Approved by:	PWG	**Date:**	5th December 2023
Last reviewed on:	March 2019		
Next review due by:	December 2026		
SLT Lead:	Business Manager		

St George Catholic College uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property.

Introduction

1. The system comprises a number of fixed and dome cameras.
2. The system does not have sound recording capability.
3. The CCTV system is owned and operated by the school, the deployment of which is determined by the school's leadership team.
4. The CCTV is monitored centrally from the IT offices by the IT technicians.
5. The school's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and UK GDPR. The use of CCTV, and the associated images and any sound recordings is covered by the Data Protection Act 2018. This policy outlines the school's use of CCTV and how it complies with the Act. Under the 2018 new GDPR we are still committed to using CCTV to keep our students and staff safe and to ensure the safety of the school site and will only use CCTV in the appropriate manner for our school.
6. All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are aware of their responsibilities under the CCTV Code of Practice (appendix A). All employees are aware of the restrictions in relation to access to and disclosure of recorded images and sound.

Statement of Intent

1. The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use.
2. CCTV warning signs will be clearly and prominently placed at all external entrances to the school, including school gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV.
3. The planning and design has endeavoured to ensure that the Scheme 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.

Siting the Cameras

1. Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.
2. The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.
3. Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

Covert Monitoring

1. The school may in exceptional circumstances set up covert monitoring. For example:
   i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
   ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.
2. In these circumstances authorisation must be obtained from a member of the senior leadership team.
3. Covert monitoring must cease following completion of an investigation.
4. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

Storage and Retention of CCTV images

1. Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.
2. All retained data will be stored securely.

Access to CCTV images

1. Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

Subject Access Requests (SAR)

1. Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.
2. All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.
3. The school will respond to requests within 40 calendar days of receiving the written request and fee.
4. A fee of £10 will charged per request.
5. The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

Access to and Disclosure of Images to Third Parties

1. There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).
2. Requests should be made in writing to the Headteacher at info@stgcc.co.uk

3. The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Complaints

Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

APPENDIX A

Surveillance Camera Code of Practice pursuant to the Protection of Freedoms Act 2012 as updated November 2022

System operators should adopt the following 12 guiding principles:

1. 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.
2. 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.
3. 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.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. 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.
6. 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.
7. 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.
8. 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.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. 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.
11. 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.
12. 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.

SAINT GEORGE CATHOLIC COLLEGE

CCTV REQUEST FORM

Alleged Incident

Name	
Reason for request	
Date and Time	
Location of Alleged Incident	
Details of alleged incident/images sought	
	Signature: ……. Job Title: ……. Date: ……. **CCTV images found and copy given** Signed …… Date …… Placed on hard drive on ……