St. Joseph's Catholic College

CCTV Policy 2019

Monitoring

By	Review Period	Method
Senior leadership team	Annual	Meeting

Ownership: Chief Financial and Operating Officer

Revision History

Review	Changes	Next Review Date
New Policy		June 2018
February 2019	Reviewed and updated	February 2020

1. Introduction

St. Joseph's Catholic College is fully committed to the safety of its staff, students and visitors and to this extent has invested in the security of its buildings and facilities. The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at the College.

Common CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under the Data Protection Act 2018. The person ultimately responsible for data protection within the College is the Principal.

The system comprises a number of fixed and dome cameras located both internally and externally around the site. All cameras may be monitored and are only available for use by approved members of staff.

The CCTV system is owned by the Academy and will be subject to review annually.

2. Objectives of the CCTV System

The objectives of the CCTV system are:

1. To protect the Academy buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption.

2. To increase the personal safety of staff, students and visitors and reduce the fear of physical abuse, intimidation and crime.

3. To support the police in a bid to deter and detect crime.

4. To assist in identifying, apprehending and prosecuting offenders on the Academy site.

5. To protect members of the public and private property.

6. To assist in the usage and management of the Academy building on a day to day basis.

7. To assist in the investigation of incidents, e.g. bullying and vandalism

3. Statement of Intent

1. The CCTV system will be registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements both of the Data Protection Act 2018 and the Commissioner's Code of Practice.

2. The Academy will comply with the Data Protection Act 2018, whether it be information, recordings and downloads which relate to the CCTV system.

3. Cameras will be used to monitor activities within the Academy buildings, the car parks and other areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the occupants within the Academy, together with its visitors.

4. Staff have been instructed to ensure that static cameras will not focus on private homes, gardens and other areas of private property.

5. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorization from the Chief Financial and Operating Officer being obtained.

6. Materials or knowledge secured as a result of CCTV system will not be used for any commercial purpose. Downloads will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Downloads will never be released to the media for purposes of entertainment.

7. The planning and design of the existing CCTV system has endeavored to ensure that the CCTV system will give maximum effectiveness and efficiency but it is not possible to guarantee that the CCTV system will cover or detect every single incident taking place in the areas of coverage.

8. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the Academy CCTV.

9. If necessary, permission will be sought from anyone else who may be identifiable before any footage is released. For example, a victim will be asked for permission before release.

4. Operation of the System

1. The system will be administered and managed by the Chief Financial and Operating Officer, in accordance with the principles and objectives expressed in this Policy.

2. The day-to-day management will be the responsibility of the Facilities Manager
3. The CCTV system will be operated 24 hours each day, every day of the year.

4. Any data recorded on the system will be retained in line with the College's Data Retention Policy and securely disposed of once the retention period has ended.

5. CCTV System

1. The Facilities Manager will check and confirm the efficiency of the system on a daily basis and in particular that the equipment is properly recording and that cameras are functional.

2. Access to the CCTV will be strictly limited to the members of staff approved by the Chief Financial and Operating Officer.

3. Unless an immediate response to events is required, staff must not direct cameras at an individual or a specific group of individuals.

4. The CCTV system may generate a certain amount of concern from members of the public. Any concern expressed by a member of the public should be referred to the Chief Financial and Operating Officer. If the member of public wishes to see CCTV footage they must apply to do so to the Chief Financial and Operating Officer Viewing must be in person, on site. If permission is granted, the member of the public must be accompanied throughout the visit by a member of staff.

5. Any site visit by a member of the public may be immediately curtailed if the operational requirements of the CCTV System make this a necessity.

6. Other administrative functions will include maintaining hard disc space, filing and maintaining occurrence and system maintenance logs by the Facilities Manager.

7. In the event of an emergency which requires an immediate contact with an emergency service to be contacted by a member of staff. The emergency procedures identified in the Health and Safety Policy will be adhered to.

6. Liaison

1. Liaison meetings may be held with all bodies involved in the support of the CCTV system i.e maintenance contractors, approved staff, police etc.

7. Monitoring Procedures

1. Camera surveillance may be maintained at all times for monitoring purposes.

2. Out of hours the system may be connected to an external Remote Video Receiving Centre (RVRC) in the event of a security alarm activation.

8. Video Download Procedures

1. Recordings may be viewed by the police for the prevention and detection of crime. Permission to do this will be given from the Chief Financial and Operating Officer or Data Protection Officer.

2. A record will be maintained of the release of downloads to the police or other authorised applicants. A register will be available for this purpose and will be kept by the Data Protection Officer.

3. Viewing of downloads by the police must be recorded in writing and in the register. Requests by the police can only be actioned under the Data Protection Act 2018.

4. Should a download be required as evidence, a copy may be released to the police under the procedures described in the above paragraphs of this Policy. Downloads will only be released to the police on the clear understanding that the disc remains the property of the College, and both the disc and information contained on it are to be treated in accordance with this Policy. The College also retains the right to refuse permission for the police to pass to any other person the disc or any part of the information contained thereon.

5. Applications received from outside bodies (e.g. solicitors, students, staff, parents and carers) to view or release downloads will be referred to the Chief Financial and Operating Officer. In these circumstances downloads will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. Requests must be made in writing. A fee of £100.00 can be charged in such circumstances.

6. Applications received from within the College (e.g. made by staff as part of the legal basis for completing tasks associated with their job) to view CCTV footage must be made on the bespoke CCTV viewing application forms. These will be referred to the Chief Financial and Operating Officer for that officer's decision whether to permit viewing.

9. Breaches of the Policy (including breaches of security)

1. Any breach of this Policy by Academy staff will be initially investigated by the Chief Financial and Operating Officer, in accordance with the Disciplinary Policy and complaints policy.

2. Any serious breach of the Policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10. Assessment of the Scheme and CCTV Usage Policy

Performance monitoring, including random operating checks, may be carried out by the approved persons.

11. Complaints

1. Any complaints about the Academy's CCTV system should be addressed to the Chief Financial and Operating Officer.

2. Complaints will be investigated in accordance with Section 9 of this Policy

12. Access by the Data Subject

1. The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

2. Requests for Data Subject Access should be made in writing to the Chief Financial and Operating Officer.

3. Requests to view any CCTV footage, must be submitted on the College CCTV request forms.

4. All subjects identifiable in the footage, must agree to the footage being released.

5. Any requests are subject to the College Data Protection Policy and any conditions contained therein. The Data Protection Policy overrules the College CCTV Policy in cases of dispute.

13. Public Information

Copies of this Policy will be available to the public, by making a request to the College. A copy of this Policy will be located on moodle information purposes to members of staff.

14. System Maintenance and Monitoring

1. The system will be maintained in accordance with the Data Protection Act 2018.

2. The system will only be maintained and monitored by companies which carry the relevant accreditation from the Security Systems and Alarm Inspection Body (SSAIB) or National Security Inspection (NSI).

3. It will be the responsibility of Facilities Manager to liaise with the maintaining company for the reporting of faults on the system, any changes to the site which

may affect the operation of the system.

4. It will be the responsibility of Facilities Manager to arrange regular system reviews with the maintaining company.

15. Summary of Key Points

- This CCTV Usage Policy will be reviewed on an annual basis.
- The CCTV system is owned and operated by the Academy.
- The CCTV system will not be manned out of hours; only external cameras will be monitored reactively by the nominated RVRC.
- The CCTV system cannot be accessed by visitors/ members of the public except by prior arrangement with the Chief Financial and Operating Officer and with good reason.
- Liaison meetings may be held with the police and other bodies.
- Copies of downloads may only be viewed by authorised staff and the police.
- Copies required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Copies will not be made available to the media for commercial or entertainment reasons.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the CCTV Usage Policy.
- Any breaches of this Policy will be investigated by the Chief Financial and Operating Officer. An independent investigation will be carried out for serious breaches.
- Breaches of the Policy and recommendations will be reported to the Chief Financial and Operating Officer.
- The system will be maintained on a regular basis by an approved contractor.

Links to other Policies
Behaviour policy
Code of Conduct
Discipline Policy
Data Protection Policy
Complaints Policy