CCTV Policy

Date approved: 23.11.15
Signed by Chair of Governors: Mr Paul Rossi

Date approved: 23.11.15
Signed by Headteacher: Mrs Kate Pereira

Reviewed: November 2020
Next Review: November 2022

St John Fisher
Catholic High School

Policy and Procedures

Contents

CCTV POLICY

Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at St John Fisher Catholic High School. The system comprises a number of fixed and dome cameras located within and around the school buildings. All cameras are controlled from the Site Office and the system can only be accessed by nominated staff. The school owns the internal CCTV system.

The Policy will be subject to review by the Governors, to include consultation as appropriate with interested parties.

CCTV Systems

1. Data Controller of the Scheme – Business Manager, St John Fisher Catholic High School, Park Lane, Peterborough, PE1 5JN.

2. The Governing Body of St John Fisher Catholic High School considers that the CCTV Scheme can contribute to security and the health and safety of pupils, staff and visitors.

3. The Headteacher and governors at the school have considered the need for using a CCTV system and have decided that it is required for the prevention of crime and for protecting the safety of students, staff and visitors to the site. It will not be used for any other purpose.

4. The general management of CCTV at St John Fisher Catholic High School is currently vested with the Business Manager.

5. The day to day management and operation of the CCTV system is the responsibility of the Site Manager.

The principal purposes of St John Fisher Catholic High School's use of CCTV:

a) To increase personal safety of students, staff and visitors and reduce the fear of crime
b) To protect the school buildings and their assets
c) To protect members of the public and private property
d) To improve security and to detect persons who are not authorised to be on the premises
e) To support Police in a bid to deter and detect crime
f) To assist in identifying, apprehending and potentially prosecuting offenders
g) To identify individuals engaged in improper conduct.

Statement of Intent

This policy has been drafted in accordance with the CCTV Code of Practice, revised edition 2008. St John Fisher Catholic High School is registered as a Data Controller with the Information Commissioner's Office in accordance with the General Data Protection Regulations 2016 (GDPR). This Policy follows the GDPR guidelines. The school will treat the system and all information, documents and recordings obtained and used as data protected by the Act.

Cameras will be used to monitor activities within the school and the grounds to identify adverse activity actually occurring, anticipated or perceived, and for the purpose of securing the safety and well being of the school's students and staff, together with its visitors.

Static cameras are positioned to ensure they do not focus on private homes, gardens and other areas of private property. At no time will a camera be directed to follow or track an individual.

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

The planning and design has endeavoured to ensure that the CCTV Scheme will give maximum effectiveness and efficiency within available means, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

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 school's CCTV system.

Siting of Cameras

1. The location of CCTV cameras is based upon a variety of information including security, health and safety and safeguarding.

2. All such CCTV equipment installed in School will only be sited in such a way that it only monitors those spaces that are intended to be covered by the equipment.

3. If domestic areas such as gardens or areas not intended to be covered by the scheme border those spaces which are intended to be covered by the equipment, then the school shall consult with the owners of such spaces if images from those spaces might be recorded. In the case of back gardens, this would be the resident of the property overlooked.

4. The employees and students will be made aware of the purpose (s) for which the scheme has been established and notices to this effect will be displayed in the school reception area and the school hall foyer. Parents will be informed through the school prospectus.

5. The operators will only use the equipment in order to achieve the purpose(s) for which it has been installed.

6. Cameras that are adjustable by the operators will not be adjusted or manipulated by them to overlook spaces which are not intended to be covered by the scheme, other than as described in 7 below.

7. If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators will be trained in recognising the privacy implications of such spaces being covered.

8. Signs, of no less than the minimum standard, will be placed so that the public are aware that they are entering a zone that is covered by CCTV.

9. Internal cameras are located in general circulation areas with the exception of the cameras located to view the washbasin areas in the student toilets to reduce vandalism. Students' privacy is not compromised by the latter.

Operation of the System

1. The CCTV system will be administered and managed by the IT (Support) team in partnership with Site team, in accordance with the CCTV Code of Practice. The day-to-day management will be the delegated responsibility of the Site Manager during the day, and the Site Officer/Assistant Caretaker on duty out of hours and at weekends.

2. The CCTV system will operate 24 hours each day, every day of the year, recording all activity.

Use of Audio

1. The CCTV Code of Practice (CoP), revised edition 2008, states that the use of audio can be justified in limited circumstances and that operators should not 'listen in'.

2. The CCTV system installed in school records visual images only and is not an audio system.

Access to Recorded Images

1. Access to the recorded images is restricted to designated members of staff some of whom will also have the authority to decide whether to allow requests for access from other individuals. See Appendix A for details.

2. Viewing of the recorded images should take place in a restricted area, for example, in the Site Office or designated member of staff's office. Other employees will not be allowed to have access to that area when a viewing is taking place.

3. A record should be kept of occasions where CCTV images are viewed and should be recorded appropriately. See Appendix B.

4. All operators and employees with access to images should be aware of the procedure that needs to be followed when accessing the recorded images.

5. All operators should be trained in their responsibilities under the Code of Practice, i.e. they should be aware of:
   - The user's security policy eg procedures to have access to recorded images;
   - The user's disclosure policy

6. The main CCTV system is in the IT (support) office and the Site Manager's office. Both are password protected and only authorised staff have passwords to gain access to recorded images. Additionally there are cameras on the computer network which are administered in the same way.

Access to Live Images

1. Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed or be capable of being viewed by anyone other than authorised persons.

2. Viewing of live images should only be carried out when there is a suspicion that improper conduct may be carried out at a particular time.

3. The privacy of staff and students going about their normal legitimate business must be respected at all times.

Quality of Images and Storage of Recorded Material

1. Upon installation an initial check will be undertaken to ensure that the equipment performs properly. Regular checks will be made thereafter to ensure that the system is operating properly.

2. Images are retained on a hard disc drive for a period of 14 calendar days. Copies can be made for investigation purposes.

3. Checks will be made to ensure the accuracy of any features such as the location of the camera and/or date and time reference. Where the time/date etc are found to be out of sync with the current time/date, the operators will take such remedial action as is continued in the operations manual to correct the error.

4. Cameras will only be situated so that they will capture images relevant to the purpose for which the scheme has been established.

5. When installing cameras, consideration will be given to the physical conditions in which the cameras are located.

6. Cameras will be properly maintained and serviced to ensure that clear images are recorded. Servicing will be carried out at least annually.

7. Cameras should be protected from vandalism in order to ensure that they remain in working order.

8. A maintenance log will be kept in the monitoring centre of the system concerned.

9. The school's Site Manager will be:
   - The person responsible for making arrangements for ensuring that a damaged camera is fixed
   - Ensuring that the camera is fixed within a specific time period
   - Monitoring the quality of the maintenance work

10. Once the retention period has expired, the images will be removed or erased.

11. Images that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.

Access to and disclosure of images to third parties

1. Access to recorded images will be restricted to those persons who need to have access in order to achieve the purpose(s) of using the equipment.

2. All access to the medium on which the images are recorded should be documented.

3. Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances. Subject to paragraph 1 above, in disclosure will be limited to the following classes of persons/agencies.

   - Law enforcement agencies, where the images recorded would assist in a specific enquiry;
   - Highways authorities in respect of traffic management matters;
   - Law enforcement agencies where the images would assist a specific criminal enquiry;
   - Prosecution Agencies;
   - Relevant legal representatives

4. All requests for access or for disclosure should be recorded, if access or disclosure is denied, the reason should be documented.

5. If access to or disclosure of the images is allowed, then the following will be documented. (Appendix C)

    - The date and time at which access was allowed or the date on which disclosure was made;
    - The identification of any third party who was allowed access or to whom disclosure was made;
    - The reason for allowing access or disclosure;
    - Location of the images
    - Any crime incident number to which images may be relevant
    - Signature of person authorised to collect the medium – where appropriate.

6. Recorded images will not be made more widely available – for example they should not be routinely made available to the media or placed on the Internet.

7. If it is intended that images will be made more widely available, that decision should be made by the Headteacher or designated member of staff and the reason for that decision should be documented.

8. If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable.

Maintenance

The CCTV systems in school are maintained by the IT (support) team and the Site team.

Breaches of the policy (including breaches of security)

The Headteacher, or senior leader acting on his behalf, will initially investigate any breach of the CCTV policy by school staff. Any serious breach of the policy will be subject to the terms of disciplinary procedures already in place.

Access by Data Subject

The GDPR provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about them, including those obtained by CCTV. Requests for Data Subject Access should be made through the Business Manager.

1. In accordance with Section 7 of the GDPR 1998 (Subject Access), an individual who believes that their image has been captured by this scheme is entitled to make a written request to the Data Controller. Upon receipt of essential information, a systems search will be conducted and subject to certain conditions, the individual will be allowed access to the personal data held.
2. All subject access requests should be referred in the first instance to the Business Manager who will liaise with the Headteacher and Site Manager.

3. All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and how such requests are to be dealt with.

4. Data subjects should be provided with a standard subject access request form, a copy of this form is attached (Appendix D).

The above form will also enquire whether the individual would be satisfied with merely viewing the images recorded. The form will also indicate that the response will be provided promptly and in any event within 40 days of receiving.

5. Individuals, at the time of any subject access request, will be given a description of the type of images recorded and retained and the purpose for which the recording and retention takes place. They should be informed of their rights as provided by the 1998 Act.

6. Prior to any authorised disclosure, the Headteacher will need to determine whether the images of another "third party" individual features in the personal data being applied for and whether these third party images are held under a duty of confidence.

7. If third party images are not to be disclosed the System Manager shall arrange for the third party images to be disguised or blurred.

8. If the Headteacher decides that a subject access request from an individual is not to be complied with, the following should be documented:

    - The identity of the individual making the request;
    - The date of the request;
    - The reason for refusing to supply the images requested;
    - The name and signature of the person making the decision.

Complaints

Any complaints about the school's CCTV system should be addressed to the Headteacher.

Reviewed by the Governors Finance and Premises Committee: November 2015

Next Review Date: November 2022 **Staff Member Responsible:** Business Manager

Appendix A

Staff authorised to operate CCTV System

The Business Manager, IT (Support) team, Site Manager and Site Officer are the only staff who have permission to operate the CCTV system.

Staff authorised to view CCTV footage / still images

Members of SLT, Heads of House, Student Support Officers, the school based PCSO and those authorised to operate the system (listed above) are the only members of staff permitted to view CCTV footage or still pictures. Persons not named above must seek authorisation from a member of SLT. This includes all members of staff and police officers. The Police are able to use footage for evidence following an incident providing prior permission has been agreed with a member of SLT.

Staff authorised to make copies of CCTV footage / still images

The IT (Support) team are authorised to access the CCTV system in order to make copies of images (stills and video footage) if requested to do so by an authorised member of staff.

Appendix B

CCTV – St John Fisher Catholic High School

Recording of Viewing by Authorised School Staff

Date and Time Image Viewed:

Date: _____ Time: _____

Name of Persons Viewing the Image:

Name	Role
_____	_____
_____	_____
_____	_____

Reason for the viewing:

_____

_____

_____

Outcome, if any, of the viewing:

_____

_____

Viewing Made By: (Signature)_____

Appendix C

CCTV – St John Fisher Catholic High School

Recording of Viewing by Third Party (e.g. Police)

Date and Time Access Allowed:

Date: _____ Time: _____

Identification of any third party who was allowed access:

_____

Names of school staff present:

_____

_____

Reason for allowing access:

_____

_____

Crime incident number if applicable:

_____

Location of the images:

_____

Signature of the person authorised to collect the medium – where appropriate:

_____

Date and time copy created for evidential purposes:

Date: _____ Time: _____

Viewing Authorised By: (Signature)_____

Appendix D

CCTV – St John Fisher Catholic High School

Form to Request Access to CCTV Images

Name: _____

Address: _____

_____

_____

_____

Telephone Number: _____

Date of Birth: _____

Date image recorded: _____

Time image recorded: _____

Please complete the details above.

The Headteacher will consider the request and respond within 7 days.

Appendix E - Location of Cameras

IP Address	Location
192.168.240.4	Block 1 Comms DVR 1
192.168.240.5	Block 1 Comms DVR 2
192.168.240.6	Block 1 Comms DVR 3
192.168.240.7	Block 1 Comms DVR 3
192.168.240.8	Block 1 Comms DVR 4
192.168.240.20	Block 1 Main Path
192.168.240.21	Block 1 Science 311 outer
192.168.240.22	Block 2A Atuim Upper
192.168.240.23	Block 2B Hall Corridor
192.168.240.24	Block 2B Student Services
192.168.240.25	Block 2A Library
192.168.240.26	Block 2B Goods In
192.168.240.27	Block 2A Reception
192.168.240.28	Block 2B Servery
192.168.240.29	Block 2B MainHall
192.168.240.30	N/A
192.168.240.31	Block 3 RM 108 External
192.168.240.32	Block 2B Main Gate
192.168.240.33	Block 4 Sports Hall
192.168.240.34	Block 2B Atrium Outside
192.168.240.35	Block 2B Atrium Lower
192.168.240.36	Block 3 RM111 External
192.168.240.37	Block 2A Lobby
192.168.240.38	Block 1 CourtYard
192.168.240.39	Block 1 Art OutSide
192.168.240.40	Block 2B Bikes
192.168.240.41	Block 2B Atrium Stairs
192.168.240.42	Block 1 Toilet
192.168.240.43	Sports Hall Entrance
192.168.240.44	Block 3 RM211
192.168.240.45	Science Back Path
192.168.240.46	Reception outer
192.168.240.47	Field
192.168.240.48	Block 3 Walkway
192.168.240.49	Block 2A Inventry Scan
192.168.240.50	Block 1 Toilets
192.168.240.51	Block 3 Toilets
192.168.240.52	Block 3 Doors Right
192.168.240.53	Block 3 Upper Stairs
192.168.240.54	Block 3 Copier
192.168.240.55	Block 3 Maths
192.168.240.56	Block 3 Doors Left

192.168.240.57	Block 3 RE
192.168.240.58	Block 3 Humanities
192.168.240.59	Block 3 ICT Rooms
192.168.240.60	Block 3 Room 103
192.168.240.61	Block 3 Lift
192.168.240.62	Block 3 Music
192.168.240.63	Block 3 Room 113
192.168.240.64	Block 3 Doors
192.168.240.65	Block 3 Room 105
192.168.240.66	Block 3 Upper Lift
192.168.240.67	Block 3 Room 211
192.168.240.68	Main Hall
192.168.240.69	Sports Hall
192.168.240.70	Block 1 Doors
192.168.240.71	Block1 307
192.168.240.72	Block 1 308
192.168.240.73	Block 1 Call Point
192.168.240.74	Block 1 RM311
192.168.240.75	Block 1 ART
192.168.240.76	Six Form
192.168.240.77	Six Form
192.168.240.78	Bike Shed
192.168.240.79	Block 2A Room 401
192.168.240.80	Block 2 A Six Form
192.168.240.81	Block 3 Room 109
192.168.240.82	Court Yard
192.168.240.83	Site
192.168.240.84	Servery
192.168.240.85	Servery