# St John Fisher Catholic College
# Closed Circuit Television Policy

| | |
|---|---|
| Date: | September 2023 |
| Adopted: | September 2023 |
| Review: | September 2024 |

## 1. Introduction

1.1 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 College, hereafter referred to as 'the School'.

1.2 The CCTV system is owned by the School.

1.3 The system comprises of internal and external cameras located in and around the school premises. Appended to this document are plans of the School showing the location of all external cameras. The monitor for internal cameras is located in the main school office and the monitor for external cameras and the system control centre are in the Premises staff office.

1.4 A CCTV camera is located in every learning space within the School as well as communal learning zones, walk-ways, main entrances and exits and external areas including car parks, play grounds and vehicle entry and exit points.

1.5 All external cameras are monitored by Premises staff and images recorded direct to the CCTV camera control unit.

1.6 This Policy follows the GDPR guidelines.

1.7 Operation of the School CCTV Policy will be reviewed annually by the Academy Committee and will include consultation, as appropriate, with interestedparties.

2. The objectives of the CCTV System are to:

- protect the School buildings and their assets;

- increase personal safety and reduce the fear of crime;
- support the Police in a bid to deter and detect crime;
- assist in identifying, apprehending and disciplining offenders;
- protect members of the public and private property whilst on school premises;
- reflect on behavioral instances of pupils;
- facilitate the identification of any activity/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

**3. Statement of Intent**

3.1 The CCTV System will be registered with the Information Commissioner's Office under the terms of the GDPR regulations and will seek to comply with the requirements both of the GDPR and the Commissioner's Code of Practice 2014 (Draft).

3.2 The School will treat the system and all information, documents and recordings obtained and used as data which are protected by GDPR.

3.3 Cameras will be used to monitor activities within all perimeter areas of the buildings to protect for arson, all classrooms and communal walk ways to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the School, together with the wellbeing of school personnel, pupils and its visitors.

3.4.1 Staff have been instructed to ensure cameras are not able to focus on private homes, gardens and other areas of private property.

3.4.2 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 authorisation being obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act, 2000.

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

3.6 The planning and design has endeavoured to ensure that the CCTV System 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.

3.7 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 CCTV.

## 4. Operation of the CCTV System

4.1 The system will be administered and managed by Vicky Bowers, in accordance with the principles and objectives expressed in this Policy.

4.2 The CCTV system will be operated 24 hours per day, 365 days per year.

## 5. Operational Control

5.1 The Operational Controller will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

5.2 The System Administrator will ensure that all staff involved with the operation of the CCTV system are properly trained and fully understand their roles and responsibilities in respect of GDPR.

a. the user's security policy (procedures to have access to recorded images);

b. the user's disclosure policy;

c. rights of individuals in relation to their recorded images.

Training records will be maintained accordingly.

5.3 Access to the viewing monitors will be strictly limited to selected senior and administrative staff together with those directly involved in the security of the School.

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

5.5 Staff, visitors and others entering areas with CCTV viewing monitors will be subject to particular arrangement as outlined below.

5.6 Authorised staff must satisfy themselves over the identity of any other visitors and the purpose of their visit.

5.7 If an emergency arises out of hours, permission must be obtained from the Headteacher to view or process recorded material.

5.8 Other operational functions will include maintaining recorded materials and hard disc space, filing and maintaining occurrence and system maintenance logs.

5.9 Incidents involving the Emergency Services must be notified to the Headteacher and Deputy Headteacher.

## 6. Liaison

Liaison meetings will be held as required with all staff involved in the support of the system.

## 7. Monitoring Procedures

7.1 Camera surveillance is to be maintained at all times.

7.2 Pictures will be continuously recorded or when activated by movement.

7.3 No covert monitoring will be undertaken until the circumstances have been considered by, and written authorisation obtained from the Headteacher.

7.4 Covert surveillance activities of law enforcement agencies are not covered here as they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000.

7.5 Prior to any request for covert surveillance to be considered, the applicant must be able to justify the request as being exceptional for the following reasons:

- the monitoring relates to behaviour, not to contract performance;
- it is carried out to investigate a suspected criminal activity or malpractice;
- informing staff is likely to prejudice the above purpose and certain standards for covert monitoring are complied with.

The standards relating to covert monitoring are satisfied if:

- specific criminal activity has been identified;
- a need to obtain evidence by covert monitoring is established;
- following assessment, it is concluded that informing employees would prejudice the gathering of evidence;
- a time period for monitoring has been identified; and
- the provisions of RIPA are complied with.

At the conclusion of any investigation, all covert cameras must be removed from their location(s) and all none relevant data destroyed as soon as possible.

## 8. Recorded Material Procedures

8.1 In order to maintain and preserve the integrity of the recorded material used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each item of recorded material must be identified by a uniquemark.
- Before use each item on which images will be recorded must be cleaned of any previous recording.
- The person making the recording shall register the date and time of recorded material insert, including recorded materialreference.
- Any recorded material required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure recorded material store. If recorded material is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence materialstore.
- If the recorded material is archived the reference must benoted.

8.2 Recorded materials may be viewed by the Police for the prevention and detection of crime, authorised officers of the Police for supervisory purposes, authorised demonstration and training.

8.3 A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register will be made available for this purpose kept by Interserve FM.

8.4 Viewing of recorded materials by the Police must be recorded in writing and in a log book. Requests by the Police can only be actioned under current GDPR regulations.

8.5 Should recorded material be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1. Recorded materials will only be released to the Police on the clear understanding that the recorded material remains the property of the school, and both the recorded material and information contained on it are to be treated in accordance with this document.

8.6 The School retains the right to refuse permission for the Police to pass to any other person the recorded material or any part of the information contained thereon. On occasions when a Court requires the release of an original recorded material this will be produced from the secure recorded material store, complete in its sealed bag.

8.7 If the Police require the School to retain the stored recorded materials for use as evidence in the future, such recorded materials will be properly indexed and properly and securely stored until they are needed by thePolice.

8.8 Applications received from outside bodies (e.g. solicitors) to view or release recorded materials will be referred to the Head Teacher. In these circumstances recorded materials 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. If there are uncertainties as to the validity of any request, clarification should be sought initially from the MAC Accounting Officer

A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

## 9. Record Keeping/Incident Logs

The School will maintain comprehensive records relating to the management of the system and incidents. Model documents from the installers/providers of CCTV system may be utilised for this purpose.

## 10. Retention of Data

10.1 There are no specific guidelines about the length of time data images should be retained. Consequently, the period of retention will be determined locally, will be documented and understood by those operating the system and will be for the minimum period necessary to meet the objectives of the CCTV scheme. A period of 30 days is considered adequate unless determined otherwise (see 10.2 below)

10.2 Where CCTV data is required to assist in the prosecution of a criminal offence, data will need to be retained until collected by the Police.

10.3 Measures to permanently delete data should be clearly understood by persons that operate the system. These may be achieved by means of regular rotation of video tape(s) to ensure old data is overwritten or adjusting the image quality on disc based systems to ensure data is overwritten after a set period.

10.4 Systematic checks should be carried out to ensure the deletion regime is strictly followed.

## 11. Breaches of the Policy (including breaches of security)

Any breach of the Policy by School staff will be initially investigated by the System Administrator to determine disciplinary action, if necessary, and to make recommendations on how to remedy the breach.

## 12. Assessment of the CCTV System

An annual assessment will be undertaken by the Head Teacher to evaluate the effectiveness of the CCTV system.

The outcome of the assessment will be reported to a meeting of the Academy Committee who will determine if the system is achieving the objectives of the scheme, or if the system requires modification.

## 13. Complaints

Any complaints about the School's CCTV system should firstly be made, in writing, to the Head Teacher. Complaints will be investigated in accordance with section 11 of this document.

## 14. Access by the Data Subject

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

If the individual is not the focus of the footage i.e. they have not been singled out or had their movements tracked then the images are not classed as 'personal data' and the individual is not entitled to the image under the provisions of Subject Access – GDPR.

14.2 Requests for Data Subject Access should be submitted via an enquiry form (see Annex A) submitted to the Head Teacher.

## 15. Public Information

Copies of this Policy will be available to the public from the School's website.

## 16. Further Information

Information and advice about the operation and maintenance of the Schools CCTV systems is available from the Premises Staff (tel: 01782 307551).

The Information Commissioners website www.ico.org.uk will contain the most up to date information and should be consulted on a regular basis to ensure all elements of this policy continue to reflect current guidance.

## 17. Summary of Key Points

17.1 The CCTV system is operated by Premises staff on behalf of the school.

17.2 The CCTV system will be reviewed annually to evaluate its effectiveness and the Academy Committee will determine if the system is achieving the objectives of the scheme or if modifications are required.

17.3 Liaison meetings may be held with the Police and other bodies when a requirement is identified.

17.4 Recorded materials will be properly indexed, stored and destroyed after an appropriate period. A period of 30 days is considered adequate unless determined otherwise.

17.5 Recorded materials may only be viewed by authorised School staff and the Police.

17.6 Recorded materials required as evidence will be properly recorded witnessed and packaged before copies are released to the Police.

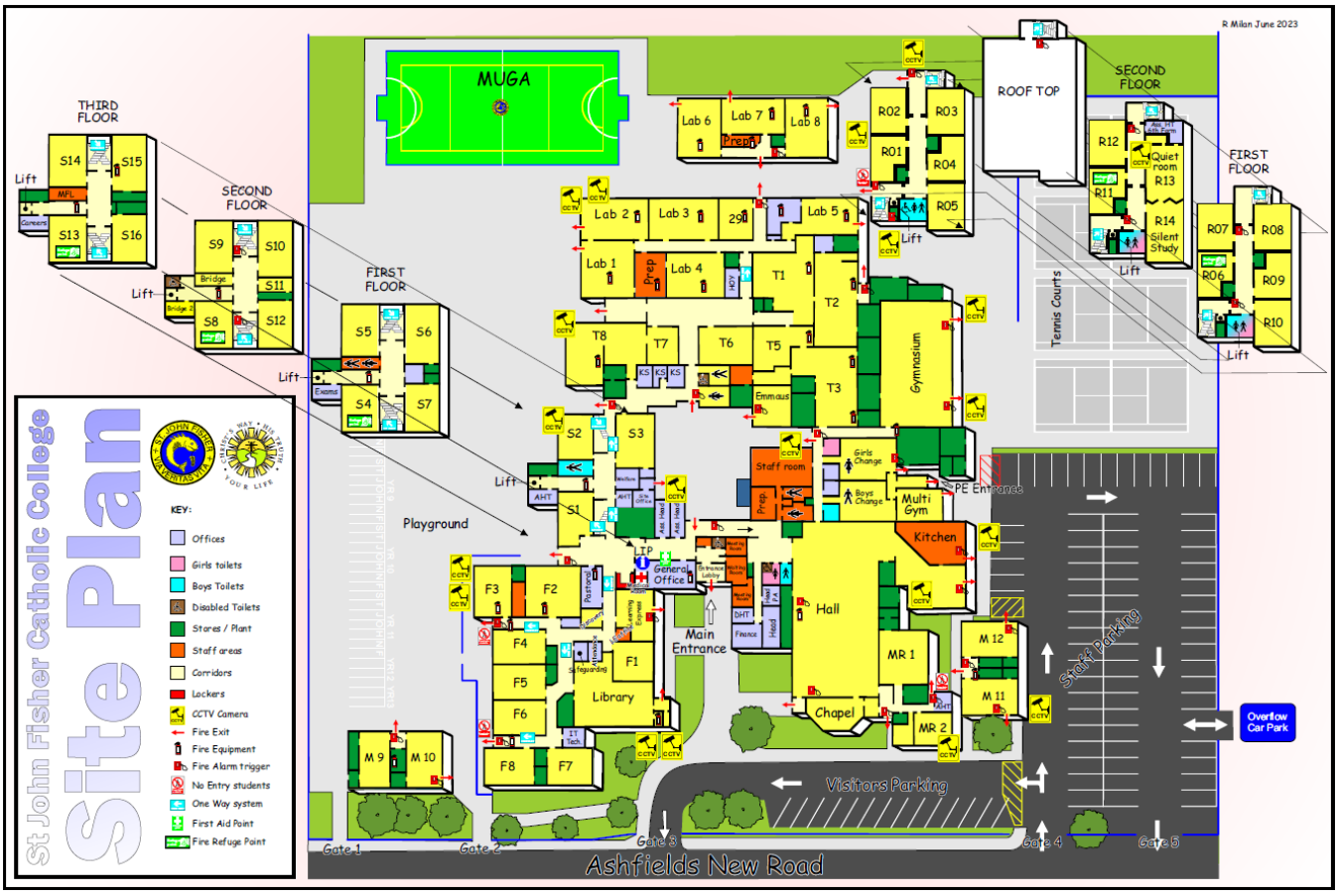
17.7 Recorded materials will not be made available to the media for commercial or entertainment purposes.

17.8 Recorded materials will be deleted from the computer hard drive after a defined period.

17.9 No covert surveillance will be undertaken without the written consent of the Corporate Director - People and the Director of Legal and Governance Services.

17.10 Breaches of this policy will be initially investigated by the System Administrator identified in Section 4.1 of this Policy to determine disciplinary action, if necessary, and to make recommendations on how to remedy the breach.

Site Plan & Camera Locations



Annex A Request for Data Subject Access

[Your full address]
[Phone number]

[The date]

St John Fisher Catholic College
Ashfields New Road
Newcastle-under-Lyme
Staffordshire
ST5 2SJ

Dear Sir or Madam

**Subject access request**

[Your full name and address and any other details to help identify you and the information you want.]

Please supply the information about me I am entitled to under the GDPR Regulations relating to: [give specific details of the information you want, for example

- CCTV camera situated at ('E' location) on 23/5/12 between 11am and 5pm;

If you need any more information from me, or a fee, please let me know as soon as possible.

It may be helpful for you to know that a request for information under the GDPR Regulations should be responded to within 40 days.

If you do not normally deal with these requests, please pass this letter to your GDPR Officer. If you need advice on dealing with this request, the Information Commissioner's Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

Yours faithfully
[Signature]