CARDINAL NEWMAN CATHOLIC SCHOOL

CCTV Policy

Dated: July 2020

Contents

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 Cardinal Newman School, hereafter referred to as 'the School'.

1.2 The CCTV system is owned by the school.

1.3 The system comprises of a number of networked cameras located in and around the school premises.

1.4 All cameras are monitored by selected senior and administrative staff together with those directly involved in the security of the school site.

1.5 This Policy follows Data Protection Act guidelines.

1.6 Operation of the School CCTV Policy will be reviewed periodically by the School Governing Body and will include consultation, as appropriate, with interested parties.

2. Objectives of the CCTV Scheme

(a) Safeguarding of pupils and staff.

(b) To protect the School buildings and their assets

(c) To assist in managing the school including behaviour management

(d) The system will not be used to monitor staff conduct or performance, except where required to investigate the alleged commission of a crime.

(e) To increase personal safety and reduce the fear of crime

(f) To support the Police in a bid to deter and detect crime

(g) To assist in identifying, apprehending and disciplining offenders

(h) To protect members of the public and private property.

3. Statement of Intent

3.1 The CCTV Scheme will be registered with the Information Commissioner, if necessary, under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice 2008.

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

3.3 Cameras will be used to monitor activities within the school and the school grounds to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the School, together with its visitors.

3.4 Cameras are not focussed on private homes, gardens and other areas of private property.

3.4.2 Cameras are not to be used for dedicated surveillance of 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 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.

3.7 Warning signs, as required by the Code of Practice of the Information Commissioner have been installed.

4. Operation of the CCTV System

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

4.2 The day-to-day management will be the responsibility of the Business Manager and The ICT Network Manager.

4.3 The CCTV system will be operated all day every day.

5. Operational Control

5.1 The Operational Controller will check and confirm the efficiency of the system weekly 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 data protection issues e.g.

(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.

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

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

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

5.6 Incidents involving the Emergency Services must be notified to the Headteacher or the Business Manager.

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

7.4 Covert surveillance activities of law enforcement agencies are not covered here because 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;

and

• 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:

(i) Access to recorded material will only granted to users with permission from the Headteacher/Business Manager.

(ii) If necessary copies will be burned to DVD or downloaded to a USB stick to pass to law enforcement agencies.

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 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 provided..

8.8 Applications received from outside bodies (e.g. solicitors) to view or release recorded materials will be referred to the Headteacher. 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 Coventry City Council Legal Services Dept.. A fee can be charged in some circumstances e.g. £10 for subject access requests.

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. Typically data shall be retained for up to 31 days unless considered evidential or deemed necessary.

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. Currently data automatically deletes after the retention period unless saved to a file on the non-networked PC.

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 (identified in section 4.1) 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 School Governors 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 Headteacher. Complaints will be investigated in accordance with section 11 of this document.

14. Access by the Data Subject

14.1 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. 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 – Data Protection Act 1998.

14.2 Requests for Data Subject Access should be submitted to the Headteacher.

15. Public Information

Copies of this Policy will be available to the public from the School Office.

16. Further Information

The Information Commissioners website www.ico.gov.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 owned and operated by the School.

17.2 The CCTV system will be reviewed annually to evaluate its effectiveness and the School Governors 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 stored for 90 days on the Hikvision system. The Mobotix system stores recorded materials for up to 12 month and is variable to individual units

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

17.6 Recorded materials required as evidence will be 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 NAS storage unit (Network-attached storage) after a defined period unless considered evidential or necessary to be kept for longer.

17.9 No covert surveillance will be undertaken without the written authority being obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act, 2000.

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.