Malbank School & Sixth Form College

CCTV Policy

Date of last review – 05/02/2018

Date of next review – 04/02/2019

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 Malbank School & Sixth Form College, hereafter referred to as 'The School'.

1.2 The CCTV system is owned by the school.

1.3 The system comprises of a mixture of analogue and digital IP 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 and will be updated, if necessary to reflect the requirements of the new General Data Protection Regulations (GDPR) which come in to effect May 2018.

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

2 Objectives of the CCTV Scheme

(a) To protect the School buildings and their assets

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

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

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

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

(f) To assist with behaviour related incidents

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 buildings, communal play areas and school car parks to Identify behaviour related issues, criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the School, together with 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 authorisation from a member of the school's Senior Leadership team 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 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 the ICT Team in accordance with the principles and objectives expressed in this Policy.

4.2 The CCTV system will be in operation 24 hours a day, 365 days a year.

5 Operational Controls

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

5.2 The ICT Network Manager 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.

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 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual Observations will not be permitted.

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

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

5.10 Incidents involving the Emergency Services must be notified to the Headteacher or Strategic Business Manager

6 Liaisons

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 Video footage will be continuously recorded or when activated by movement.

7.3 No covert monitoring will be undertaken until the circumstances have been considered by the Headteacher or Strategic Business Manager

7.4 Prior to any request for covert surveillance to be considered, the applicant must be able to justify the request as being exceptional such as:

- The monitoring relates to behaviour;
- 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 The Regulation of Investigatory Powers Act 2000 (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) Each item of recorded material must be identified by a unique mark.

(ii) Before use each item on which images will be recorded must be cleaned of any previous recording.

(iii) The person making the recording shall register the date and time of recorded material insert, including recorded material reference.

(iv) Recorded material required for evidential purposes must be sealed, witnessed, signed by a member of the ICT Team, 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 material store. Approval must be obtained from the Headteacher or Strategic Business Manager prior to releasing any recorded material to the Police.

(v) If the recorded material is archived the reference must be noted.

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.

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 Section 29 of the Data Protection Act, 1998.

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(iv). 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 is 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 the Police.

9 Record Keeping/Incident Logs

The School will maintain adequate and comprehensive records relating to the management of the system and incidents.

10 Retention of Data

10.1 The period of retention as determined by the school is 7 days, this will be documented and understood by those operating the system and will be necessary to meet the objectives of the CCTV Scheme.

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 CCTV data for each camera will be stored on a hard drive for 7 days. After this period the CCTV system will start to overwrite the data as a rolling program. At any one time only 7 days footage will be available.

10.4 Systematic checks will 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 or Strategic Business Manager (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 Headteacher or Strategic Business Manager 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.

15 Public Information

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

16 Summary of Key Points

16.1 The CCTV system is owned and operated by the School.

16.2 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.

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

16.4 Recorded materials will be properly indexed, stored and destroyed after an appropriate period. A period of 7 days has been determined by the school. 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.

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

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

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

16.8 Recorded materials will be deleted from the computer hard drive after a period of 7 days as determined by the school.

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