St Mary's CE High School

'Aspire - Challenge - Succeed'

CCTV System Policy

Summer 2018

Academy Company Reg.No 07999861

"Our vision, as a school with a Christian ethos, is founded on The Parable of the Sower, where

***"Through God's love, we are the rich soil where seeds flourish and roots grow"**, Mark 4: 3-9*

*This underpins our motto, **Aspire Challenge Succeed**, and is key to what we do. We provide a safe, nurturing environment in which we can all flourish. We have the very highest aspirations for our students, their families, our local community, and ourselves. We challenge students by having a rich and exciting curriculum provision and by making learning practical, engaging and enjoyable. We enable students to succeed by providing the best possible personalised support."*

Nicholas Simms – Head Teacher

St Mary's CE High School
CCTV System Policy

The Governing body is committed to securing the safety and well-being of employees, students and others affected by activities on school premises. The Governors of St Mary's have made safeguarding a fundamental priority and are committed to ensuring that safeguarding of children and young people remains at the core of their work. For this reason, the principles of excellent safeguarding practice are integral to the culture of St Mary's and every aspect of the school and trading company's work. This policy supports this commitment to safeguarding and should be read in conjunction with other school and trading company policies as appropriate.

It is every person's responsibility to safeguard and promote the welfare of children and it remains a paramount concern of all who work in and who are part of the St Mary's community.

Aims

- To provide a safe environment for staff and students
- To provide improved site security
- To prevent and identify vandalism and theft
- To prevent anti-social behaviour in areas around the school
- To ensure the health and safety of the staff, students and visitors to the School

1. Introduction

The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at St Mary's CE High School ('the school'). This policy is to be read in conjunction with the Code of Practice issued by the Information Commissioners and other polices relating to safeguarding, GDPR and data protection.

The system comprises a number of fixed and dome cameras located around the school site. All cameras record to devices located in the various plant rooms around the school. These are monitored in the Site Team Leader's office. Recorded images can be viewed in the Site Team Leader's office or IT office but only with express permission of a member of SLT. Live images will generally only be viewed in the Site Team Leader's office.

This policy is in line with the General Data Protection Regulations (GDPR) and will be subject to review every three years.

The CCTV system is owned by the school.

2. Objectives of the CCTV Scheme

- To assist in managing the school
- To protect the school buildings and their assets

- To increase personal safety and reduce the fear of crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To support the Police in a bid to deter and detect crime

3. Statement of intent

The CCTV scheme is already registered with the Information Commissioner and complies with the requirements both of the GDPR and the Commissioner's Code of Practice https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

The system, information, documentation and recordings obtained, will be treated in accordance with the GDPR.

Cameras will be used to monitor activities externally around the school site and internally in school buildings and in communal and public areas eg courtyard. This is for the primary purpose of ensuring the safety and well-being of the school and its visitors, which includes those utilising the school facilities as hirers. It is also intended to be used to identify criminal activity occurring, anticipated, or perceived and the positions and areas monitored reflect all of these purposes.

The cameras will not focus on any area that would intrude on personal or sensitive activity for example on toilet cubicles or in the first aid room. The school cameras will not focus on private homes, gardens and other areas of private property and through the careful positioning of the cameras, minimal collateral intrusion is anticipated.

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 written authorisation being obtained from the Head Teacher for directed surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Copies will only be released to the media by the Head Teacher for use in the investigation of a specific crime and with the written authority of the police. DVDs, USBs or images sent will never be released to the media or any other person without written consent from the Head Teacher or Police.

The planning and design has endeavoured to ensure that the 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.

Warning signs, as required to be displayed by the Information Commissioners, have been placed at all access routes to areas covered by the school CCTV. The warning signs will be checked on a regular basis and any warning sign destroyed or damaged will be replaced.

4. Operations of the system

The scheme will be administered and managed by the Head Teacher, in accordance with the principles and objectives expressed in this policy.

The day-to-day management will be the responsibility of both the Site Team Leader and the ICT Manager. The Site Team will have operational responsibility for the system during the day, out of hours and at weekends.

The CCTV system will be operational 24 hours each day, every day of the year.

The Site Team Leader and the ICT Manager will check and confirm the efficiency of the system regularly, and in particular that the equipment is properly recording and that cameras are functional.

If the need for maintenance arises the Site Team Lead will arrange this and must be satisfied of the identity and purpose of contractors before allowing entry.

Other administrative functions carried out by the Site Team Leader and ICT Technician team, will include maintaining DVD and hard drive space, filing and maintaining occurrence and system maintenance logs, as necessary.

5. Monitoring procedures

Camera surveillance is not limited to particular times of the day and can be viewed at any time.

Cameras are monitored in the Site Team offices but access to the system can be made on any suitable desk top computer once provided with sufficient access and only once authorised by a member of SLT.

If covert surveillance is planned or has taken place, only the Head Teacher or the Police are able to authorise such use and it must be used in accordance with the aims and objectives of the policy.

The footage is only stored on the system's hard drive for an average maximum of 31 days unless it has been saved onto an external hard drive for a specific purpose eg an investigation, (at which point it will be saved for as long as the investigation is being carried out/until the matter is fully resolved).

Footage which has been saved will be disposed of securely eg shredded, in line with our Data Retention Policy.

6. Viewing footage and DVD/USB/Image procedures

If a copy of an incident or event is recorded from the hard drive onto a Network area, DVD or USB or an image is retained and in order to maintain and preserve the integrity of the DVD/USB/Image, the following procedures for their use and retention must be strictly adhered to:

(i) Each DVD/USB/Image must be identified by a unique sequential reference

(ii) A new DVD/USB must be used before recording on to it

(iii) A register shall be kept of each DVD/USB recorded or Image supplied.

If a DVD/USB/Image is made, then this may be viewed by the Police for the prevention and detection of crime with prior permission given by the Head Teacher or Deputy Head Teacher in their absence

A record will be maintained of the release of DVDs to the Police or other authorised applicants by the Site Team Leader, for the purposes of:

1) The prevention and detection of crime
2) The apprehension and prosecution of offenders

DVDs/USBs/Images will only be released to the Police on the clear understanding that the DVD/USB/Image remains the property of the school, and both the DVDs/USBs/Images and information contained on it are to be treated in accordance with this policy and in line with the principles of GDPR. The school also retains the right to refuse permission for the Police to pass to any other person the DVD/USB/Image or any part of the information contained thereon.

The Police may require the school to retain the DVD/USB/Image for possible use as evidence in the future. Such requests will be properly indexed and securely stored in the school safe until they are needed by the Police.

Applications received from outside bodies (e.g. solicitors or hirers) to view CCTV footage or release DVDs/USBs/Images, will be referred to the Head Teacher. In these circumstances, either viewing the footage or compiling a DVD/USB or saving an image will normally only be allowed or released where satisfactory documentary evidence is produced showing that they are required for either legal proceedings, they are part of a subject access request, or are in response to a Court Order.

The provision of any information will be managed in accordance with the School's Data Protection Policy, a copy of which is available on request.

7. Breaches of the code (including breaches of security)

Any breach of this policy by school staff will be initially investigated by the Head Teacher (or duly nominated person), in order for them to take the appropriate disciplinary action.

Any personal data breach will be managed in accordance with the School's Data Breach Policy, a copy of which is available on request.

8. Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, may be carried out by The Site Team Leader and the ICT Manager. Section 8 of the Information Commissioners Code of Practice, is to be read in conjunction with this policy.

9. Complaints

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

Complaints will be investigated in accordance the School's complaints procedures and policies relating to data protection/GDPR all of which are to be read in conjunction with this policy.

10. Access by the Data Subject

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

Requests for Data Subject Access should be made to the Head Teacher.

11. Public information

Copies of this Policy will be available to the public via the school website.

12. Legal Requirements

The use of CCTV at the school has already been registered with the Information Commissioner in compliance with GDPR

Signs have been placed at each block entrance to the school, stating that CCTV is in operation.

In addition to this, smaller signs indicating the use of CCTV have been installed around the school.

Summary of Key Points

- This policy will be reviewed every three years
- The CCTV system is owned and operated by the school
- The system will not be routinely actively monitored
- DVDs/USBs/Images will be used properly, indexed, stored and destroyed after appropriate use
- DVDs/USBs/Images and hard drive footage may only be viewed by persons authorised by the school or other appropriate authority
- DVDs/USBs/Images required as evidence will be properly recorded, witnessed and packaged before copies are released to the Police
- DVDs/USBs/Images will not be made available to the media for commercial or entertainment purposes
- DVDs/USBs/Images will be disposed of securely eg shredding

- Any covert surveillance or use of a Covert Human Intelligence Source (CHIS) being considered or planned as part of an operation must comply with any corporate policies and procedures and be authorised by the Head Teacher or Police. Further legal advice however, should be obtained prior to undertaking any covert operation utilising the CCTV system
- Any breaches of this policy will be investigated by the Head Teacher. An independent investigation will be carried out for serious breaches
- Breaches of the policy and remedies will be reported to the Head Teacher

May 2018