Perton Middle School

CCTV Policy

"The Use of Closed-Circuit Television (CCTV) To Comply with the Data Protection Act 1998", The regulation of Investigatory Powers Act 2000 and the Protection of Freedoms Act 2012. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Contents:

Reviewed: January 2020
Review Officer: Mr N Eveson

Review Date: January 2021

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Perton Middle School, hereafter referred to as 'the school'.

This policy follows the Data Protection Act guidelines:

Information held by the school that is about individuals is covered by the Data Protection Act 2018 (DPA) and CCTV 1998, the guidance in this policy will help operators comply with their legal obligations under the DPA. The school is the Data Controller for the pupil, any educational recording and personal data.

The system comprises a number of cameras located internally and externally in and on the school building. All cameras are monitored under restricted access from passwords available to nominated Senior Leaders, In this school The Pastoral Manager, the Deputy Head Teacher and the IT Manager.

This Code follows Data Protection Act guidelines and ICO guidelines. The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.

The CCTV system is owned by the school and serviced by the schools ICT Technician department.

Objectives of the CCTV scheme

1. To increase personal safety of staff, students and visitors and reduce the fear of crime
2. To protect the school buildings and their assets
3. To support the Police in a bid to deter and detect crime
4. To assist in identifying, apprehending and prosecuting offenders
5. To protect members of the public and private property

The basic legal requirement is to comply with the DPA itself. This policy sets out the main Information Commissioner's recommendations on how the legal requirements of the DPA can be met.

The recommendations in this policy are all based on the legally enforceable data protection Principles that lie at the heart of the DPA and they have been set out to follow the lifecycle and practical operation of CCTV.

Following the recommendations in this code the school will:

- Help ensure that those capturing images of individuals comply with the DPA
- Mean that the images that are captured are usable; and
- re-assure those whose images are being captured.

This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Act in response to the use of CCTV surveillance systems.

2. 12 guiding principles

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

3. General Information

This policy takes into account:

- The Data Protection Act 1998;
- Protections of Freedoms Act (POFA) June 2013
- Freedom of Information Act 2000
- ICO Surveillance Camera Code of Practice
- The Data Protection Act 2018 (GDPR)
- The CCTV Code of Practice produced by the Information Commissioners Office;
- The Human Rights Act of 1998;
- The Regulation of Investigatory Powers Act 2000;
- The Caldicott Report 1997.

The Data Protection Act 2018 has added some subtle differences in guidance; however, the principles of the 1998 Data Protection Act that came into force on the 1st March 2000 more readily covers the processing of images of individuals caught by CCTV cameras. The changes in data protection legislation mean that for the first time legally enforceable standards will apply to the collection and processing of images relating to individuals. This policy will be updated to reflect any changes to law.

An important new feature of the legislation is the CCTV Code of Practice which sets out the measures which must be adopted to comply with the Data Protection Act 2018. This goes on to set out guidance for the following of good data protection practice. The code of practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place.

This policy will cover all employees of the school, pupils, persons providing a service to the school, visitors and all other persons whose image (s) may be captured by the system.

- The CCTV Cameras are constantly recording, there are 20 cameras in total using the Hikvision systems, all located in prominent positions around the school;
- Under the Data Protection Act we are not allowed to show any recorded footage to any person who is not a member of staff, a member of the Police Force or a council officer following the set procedures.

The person who has been appointed to oversee the system and procedures i.e. the System Manager is Mr Neil Eveson. Their position in the school is: Federation Business & Operations Manager. In their time away from school i.e. holiday, sickness, the Federation Networks Manager, Mr David Buckley will cover these duties. Mr Mike Stackhouse (ICT Team), aided by Mr Neil Rowley (pastoral manager) will control images produced and operation of the system. If images are viewed there will always be two members of staff present.

All cameras only view the school premises (internally and externally) this also considers the neighbouring houses and gardens and the cameras are fixed so at no times are these under surveillance.

This will apply no matter which camera function is employed. A hard drive is available to view the images showing the camera functions. This can only be viewed on request to the System Manager.

4. Definitions

Prior to considering compliance with the principles of the Data Protection Act a user of CCTV or similar surveillance equipment, will need to determine two issues:

The type or data being processed i.e. is there any personal data which falls within the definition of sensitive personal data as defined by the act.

Sensitive personal data includes:

- Gender
- Ethnic origin or race
- Political opinion
- Religious beliefs
- Trade Union membership
- Health – mental or physical
- Sexual life
- Commission of any offence
- Any court proceedings or findings to determine the purpose for which both personal and sensitive personal data is being processed.

The data must be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than necessary
- Processed in accordance with individuals' rights'
- Not transferred to countries without adequate protection

The information commissioner will consider the extent to which users of CCTV and similar surveillance equipment have complied with this code of practice when determining whether they have met their legal obligations when exercising their powers of enforcement.

5. Policy

Due to schools being a separate legal identity, the Head Teacher and Board of Governors are responsible for the legal compliance of the act. This will be monitored by the Data Controller (System Manager and their deputies) who has the responsibility for the day to day compliance.

The purpose of the CCTV scheme is for the:

- Prevention or detection of crime and disorder
- To prevent bullying in and around school
- Protection of pupils and employees
- To support legal cases or fraud
- Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)
- Interest of pupil, employee and public health & safety
- Protection of the schools property and assets
- To increase personal safety and reduce the fear of crime
- To assist managing the school.

The CCTV Scheme is registered with the Information Commissioner 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. The school will treat the system and all information, documents and recordings obtained and used as data which is protected by the Act.

Cameras will be used to monitor activities within the school and its car parks and other public areas 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 its visitors.

The System Manager has been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.

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 using the school's forms 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. Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police.

Information will never be released to the media for purposes of entertainment. The planning and design have 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 by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the school CCTV.

The CCTV system will be operated 24 hours each day, every day of the year.
The System Manager or their deputies will check and confirm the efficiency of the system on a weekly basis and in particular that the equipment is properly recording and that cameras are functional. (Appendix One).

Access to the CCTV facilities will be strictly limited to the System Manager and his deputies. The System managers must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused.

If out of hours emergency maintenance arises, the System Managers must be satisfied of the identity and purpose of contractors before allowing entry.
Full details of visitors including time/data of entry and exit will be recorded. When not manned the facility must be kept secured by using the password protected control.

The System Manager or his deputies must adhere to administrative functions which include maintaining hard disc space, filing and maintaining occurrence and system maintenance logs.

Emergency procedures will be used in appropriate cases to call the Emergency Services. Any breach of the Code of Practice by school staff will be initially investigated by the System Manager, in order for him to take the appropriate disciplinary action. Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

Recorded material will be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded by the CCTV system are protected and that the material can be used as evidence in court

6. Freedom of information

As we are a public school we may receive requests under the Freedom of Information Act 2000 (FOIA) Public authorities should have a member of staff who is responsible for responding to freedom of information. (Please see the Freedom of Information Folder).

Staff operating the CCTV system also need to be aware of two further rights that individuals have under the DPA. They need to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage, or and one to prevent automated decision-taking in relation to the individual. Experience has shown that the operators of CCTV systems are highly unlikely to receive such requests.

7. Fitting the Cameras

It is essential that the location of the equipment be carefully considered, because the way in which images are captured will need to comply with the Data Protection Act, to ensure this, the School will always use technicians under the guidance of the Network manager for installation.

All camera are located in prominent positions within the public and staff view and do not infringe on any privacy laws. All CCTV surveillance is automatically recorded and any breach of these Codes of Practice will be detected via controlled access to the system and auditing of the system.

Signs have been erected on all entrance points to School premises and throughout the site to ensure visitors are aware they are entering an area covered by CCTV surveillance and equipment. Signs include details of the purpose, organisation and contact details.

Use of any covert CCTV surveillance if required will be requested through the Police.

Any contractors fitting systems who may have access to confidential images/files will be asked to sign the schools Data protection form.

8. Quality of the Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose for which they are intended. This is why it is essential that the purpose of the scheme be clearly identified. For example, if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose. Images are currently recorded in 1080P quality.

All camera installations and service contracts will be undertaken by an approved Contractor or the schools Network Manager. Upon installation, all equipment is tested to ensure that only the designated areas are monitored and high-quality

pictures are available in live and playback mode. All CCTV will be serviced and maintained on an annual basis.

The system currently has 20 cameras, recording to hard drive. These cameras are currently monitored by a chosen individual with password access from a hard drive with recording and monitoring facilities.

9. Processing the Image

Images, which are not required for the purpose for which the equipment is being used, should not be retained for longer than necessary, currently the system automatically erases images after one month. While images are retained, it is essential their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. For images that need to be copied please see (Appendix 2)

10. Access to the Images by Third Parties

It is important that access to and disclosure of the images recorded by CCTV is restricted and controlled. This will ensure the rights of the individuals are preserved, but also to ensure that the continuity of evidence remains intact should the images be required for evidential purposes. (Appendix 3).

Access to the information is restricted to the System Manager and their deputies, they will only allow access following this procedure and with the appropriate forms filled in.

11. Image storage procedures

The hard drive is located in a secure, triple locked environment. In order to maintain and preserve the integrity of the system 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 disc must be identified by a unique reference number.
- Before using each disc must be cleared of any previous recording.
- The person responsible for recording will register the date and time of disc recording, including the unique reference number.
- A disc required for evidential purposes must be sealed, witnessed, signed by the person responsible for recording, dated and stored in the safe. If a disc 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 responsible member of staff, dated and returned to the safe.

- If the disc is archived the reference must be noted.
- Discs may be viewed by the Police for the prevention and detection of crime.
- A record will be maintained of the release of discs to the Police or other authorised applicants. A register will be available for this purpose.
- Viewing of discs by the Police or any external individual must be recorded in writing.
- Any images sent over the internet will be sent from and received, only to an encrypted receiver. A password will be sent to gain access to the image to ensure security. This will then be entered in the register.

(Requests by the Police can only be authorised under section 29 of the Data Protection Act 1998. Should a disc be required as evidence, a copy may be released to the Police under the procedures described in paragraph 10 of this Code. Discs will only be released to the Police on the clear understanding that the disc remains the property of the school, and both the disc and information contained on it are to be treated in accordance with this code).

The school also retains the right to refuse permission for the Police to pass to any other person the disc or any part of the information contained thereon. On occasions when a Court requires the release of an original disc this will be produced from the safe, complete in its sealed bag. The Police may require the school to retain the stored discs for possible use as evidence in the future. Such discs will be properly indexed and properly and securely stored until they are needed by the Police. Applications received from outside bodies (e.g. solicitors) to view or release discs will be referred to the Head teacher. In these circumstances' discs 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. This must be provided within 40 calendar days of receiving the required fee of £10 and the request.

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

Any breach of the Code of Practice by school staff will be initially investigated by the Head teacher and Governing Body, in order for them to take the appropriate disciplinary action. Complaints will be dealt with in accordance with the ICO Code of Practice.

13. Complaints

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

Business & Operations Manager. Complaints will be investigated in accordance with the ICO Code of Practice.

14. Access by individuals/Data Subject

Section 7 of the 1998 DPA gives any individual the right to request CCTV images. Individuals who request access to images must be issued an access request form.

Upon receipt of the completed form the security manager will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. If the duty of care cannot be discharged then the request can be refused. (Appendix Four).

The CCTV system is owned and operated by the school. The Control system is not open to visitors except by prior arrangement and good reason. Liaison meetings may be held with the Police and other bodies. Any recordings will be used properly, indexed, stored and destroyed after appropriate use.

Recordings may only be viewed by Authorised School Officers and the Police. Recordings required as evidence will be properly recorded witnessed and packaged before copies are released to the Police. Copies will be disposed of securely by incineration. Any breaches of this Code will be investigated by the System Manager. An independent investigation will be carried out for serious breaches.

Breaches of the Code and remedies will be reported to the Head Teacher and the Governors. Staff using the CCTV system or images will be trained to ensure they comply with this code.

Training will be offered to staff, which will include the following:

- awareness of the Schools Policy;
- details on how the school records images and how they secure them;
- who to contact if they receive a request for data;
- the sanctions in place should there be a security breach;
- the awareness to staff that they are committing a crime if they misuse CCTV equipment.

15. The Data Protection Act

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.

Data protection principles: The CCTV usage is governed under the 8 principles of the Data Protection Act. (Please see the Data Protection Policy)
Data Subject Access Requests should be made in writing to the Head teacher. The request should provide as much information as possible to enable the school to find the images including date, time and location. If the Data Subject is unknown to the school then a photograph of the individual and/or a description of what they were wearing at the time they believe they were caught on the system may be requested in order to aid identification.

Copies of this Code of Practice will be available to the public from the School Office and the school website.

16. Summary of Key Points

- This Code of Practice will be reviewed every year.
- The CCTV system is owned and operated by the school.
- Liaison meetings may be held with the Police and other bodies.
- Recording discs used will be properly indexed, stored and destroyed after appropriate use.
- Discs may only be viewed by Authorised School staff and the Police.
- Discs required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Discs will not be made available to the media for commercial or entertainment.
- Discs will be disposed of securely by incineration.
- Any breaches of this code will be investigated by the Head teacher. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Head teacher.

17. Contacts

System Manager – Mr Neil Eveson 01902 907560
Network Manager – Mr David Buckley 01902 907560
IT Manager On-site – Mr Mike Stackhouse 01902 758244
Staffordshire County Council Information Officer – Mrs Hedda Motherwell

18. Appendices

Appendix One - Weekly Check List
Appendix Two - Taking and Copying Images
Appendix Three - Access by Third Parties
Appendix Four - CCTV Request Form