



DORMSTON SCHOOL

CCTV Policy

“The Use of Closed Circuit Television (CCTV) To Comply With the Data Protection Act 1998”

Contents:

1. Introduction
2. General Information
3. Definitions
4. Policy
5. Freedom of Information
6. Fitting the Cameras
7. Quality of the Images
8. Processing the Image
9. Access by Third Parties
10. Access by Individuals
11. Data Protection Act
12. Contacts
13. Appendix

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at The Dormston 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 1998 (DPA) and 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 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 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. General Information

This policy takes into account:

- ✓ the Data Protection Act 1998;
- ✓ the CCTV Code of Practice produced by the Information Commissioners Office;
- ✓ the Human Rights Act of 1998;
- ✓ the Regulation of Investigatory Powers Act 2000;
- ✓ Caldicott Report 1997.

The Data Protection Act 1998 came into force on the 1st March 2000 and contains broader definitions than those of its predecessors (1984) Act and 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.

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 1998. 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 27 cameras in total, 14 internal and 13 external using the Milestone and MX Control 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 or a member of the Police Force following the set procedures.

The person who has been appointed to oversee the system and procedures i.e. the System Manager is Mr Simon Carroll. Their position in the school is: Deputy Head Teacher. In their time away from school i.e. holiday, sickness, the School Business Manager Mr Neil Eveson will cover these duties. Mr Sneal Tak (ICT Manager) will control images produced and operation of the system.

All cameras only view the school premises this also takes into account 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.

3. 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 take into account 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.

4. 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;
- ✓ 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 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 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 Manger 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 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

5. 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 needs to be aware of two further rights that individual 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.

6. 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 a certified contractor 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 must include details on the purpose, organisation and contact details.

Use of any covert CCTV surveillance if required should 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.

7. 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.

All camera installations and service contracts will be undertaken by an approved contractor. 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 should be serviced and maintained on an annual basis.

The system currently has 27 cameras, recording to hard drive. These cameras are currently monitored in the Pastoral Managers office with recording and monitoring facilities.

8. 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 14 days. 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)

9. 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.

10. Access by individuals

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).

This Code of Practice will be reviewed every year.

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.

11. The Data Protection Act 1998:

Data protection principles: The CCTV usage is governed under the 8 principles of the Data Protection Act. (Please see the Data Protection Policy)

12. Main Contacts

System Manager - Mr Simon Carroll
Dudley Information Officer - Mr Lewis Bourne
Governor Responsible for Information Governance - Mr Tony Proctor

13. Appendices

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