GUISELEY
SCHOOL

A THINKING SCHOOL

CCTV Policy

Approved on:	06 December 2016
Reviewed on:	05 December 2017
Next Review:	Autumn 2018
Governors' Committee:	Resources
Responsible Officer:	Director of Admin & Finance

This policy has been drafted in accordance with the Information Commissioner's Office 'In the picture: a data protection code of practice for surveillance cameras and personal information' version1.1 issued 21/05/2015.

Guiseley School is registered as a Data Controller with the Information Commissioner's Office in accordance with the Data Protection Act 1998 (DPA).

Contents

Introduction 3
1. Impact Assessment 3
1.1. The principal purposes of Guiseley School's use of CCTV: 3
1.2. The use of CCTV must have limited impact on people's privacy 3
1.3. The benefits of having a CCTV system 3
2. Siting of Cameras 4
3. Use of Audio 4
4. Access to Recorded Images 4
5. Access to Live Images 5
6. Storage of Recorded Material 5
7. Maintenance 6
8. Subject Access Requests 6
9. Responsibility for the Operation of the CCTV System 7
Appendix I 8
The Data Protection Act 1998: data protection principles 8
Appendix II 9
The guiding principles of the Surveillance Camera Code of Practice 9

Introduction

The Information Commissioner's Office (ICO) issued its first code of practice under the Data Protection Act 1998 (DPA) covering the use of CTV in 2000. The code was developed to explain the legal requirements operators of surveillance cameras were required to meet under the Act and promote best practice. The data protection principles from the DPA 1998 are contained in Appendix I to this policy.

The unwarranted use of CCTV and other forms of surveillance cameras has led to a strengthening of the regulatory landscape through the passing of the Protection of Freedoms Act (POFA). The POFA has seen the introduction of a new surveillance camera code issued by the Secretary of State since June 2013 and the appointment of a Surveillance Camera Commissioner to promote the code and review its operation and impact. The ICO has contributed to this tougher regulatory landscape by taking enforcement action to restrict the unwarranted and excessive use of increasingly powerful and affordable surveillance technologies.

The basic legal requirement is to comply with the DPA, however the code also refers to the Freedom of Information Act 2000 (FOIA), the Protection of Freedoms Act (POFA), the Human Rights Act 1998 (HRS) and the Surveillance Camera Code of Practice issued under the POFA.

The POFA has an important regulatory role, creating the role of 'Surveillance Camera Commissioner' which has a memorandum of understanding with the ICO. The Surveillance Camera Commissioner is charged with promoting good practice and to encourage compliance with the POFA code. The POFA code is useful when the issue is not a data protection one. There are twelve guiding principles of the POFA Surveillance Camera Code of Practice. These are contained in Appendix II to this policy.

1. Impact Assessment

1.1. The principal purposes of Guiseley School's use of CCTV:

1.1.1. Safeguarding. To reduce the likelihood of students, staff or visitors becoming harmed or injured, whilst moving around the School, by persons unknown or by other students.
1.1.2. Protection of property, both that of the School and of students and staff.
1.1.3. To identify individuals engaged in improper conduct.
1.1.4. Where necessary to pass images on to the police and other relevant bodies.
1.1.5. To improve security and to detect persons who are not authorised to be on the premises.
1.1.6. To act as a deterrent.

1.2. The use of CCTV must have limited impact on people's privacy

1.2.1. Cameras are located in positions which do not adversely affect the privacy of any individual going about their normal business on the School's premises.
1.2.2. Access to live and recorded images are strictly limited to certain individuals. See sections 4 and 5 below.
1.2.3. There are signs around School advising that CCTV is in operation.

1.3. The benefits of having a CCTV system

1.3.1. Staff and students are reassured that the likelihood of them coming to harm or being injured is reduced.

1.3.2. Staff and students are reassured that if there is an incident, there is a strong possibility that the perpetrator will be identified.
1.3.3. In more serious cases, the police will have access to potentially important evidence.
1.3.4. Cameras to some extent act as a deterrent to improper behaviour.
1.3.5. Supports the School's positive behaviour policy.

2. Siting of Cameras

2.1. The location of cameras has been carefully chosen.
2.2. Internally most cameras are located in general circulation areas.
2.3. Other cameras are located within student toilet areas but only view areas where students' privacy is not affected.
2.4. Cameras in the Student Support Centre are located in every room.
2.5. There are cameras in the five ICT classrooms and the server room in the maths block.
2.6. External cameras are located to cover areas where there is a greater likelihood of inappropriate behaviour.
2.7. External cameras do not overlook areas where the general public can be seen.

3. Use of Audio

3.1. The Information Commissioner's Office 'In the picture: a data protection code of practice for surveillance cameras and personal information' version1.1 issued 21/05/2015 states that the use of audio recording, particularly where it is continuous, will, in most situations, be considered more privacy intrusive than purely visual recording. Its use will therefore require much greater justification.
3.2. Where audio recording is used it should be made clear to data subjects that audio recording is taking place, over and above any visual recording which is already occurring.
3.3. Operators should not 'listen in' to conversations.
3.4. Guiseley School considers that the use of audio in parts of the 'ARCC' is justified for the added protection of staff and students. This will be in the 'Respect' and 'Care' rooms only.
3.5. The facility to use audio recording is available in the foyer area of the Student Support Centre. Governors have decided that this facility will be switched off.

4. Access to Recorded Images

4.1. Access to recorded images should be strictly limited to the CCTV operators, Leadership Team, Key Stage Co-ordinators (KSCs), Progress and Achievement Leaders (PALs), Director of Inclusion and Behaviour Support Workers (BSWs).
4.2. All members of the School's premises team are CCTV operators (THB, ARW, PE, SSS).
4.3. In exceptional circumstances this can be extended to other relevant members of staff to identify individuals, but this must be with the permission of the relevant Leadership Team member or Key Stage Co-ordinator.
4.4. In the 6th form office, access to recorded images is also allowed for the Head and Deputy Head of the 6th form.
4.5. Viewing of recorded images must be on a 'need to see' basis.

4.6. The privacy of staff and students in the recorded images who are going about their normal legitimate business must be respected at all times.
4.7. From time to time recorded images may need to be downloaded to disc or memory stick for evidence purposes and handed to the police. Authority to do this must be restricted to two persons, namely the Facilities Manager and the Site Supervisor. A form DP7 is required from the police before images can be handed over.
4.8. The main CCTV system in the Site Supervisor's office is password protected and only premises staff and the Director of Administration and Finance have a password to gain access to recorded images.
4.9. CCTV images are also networked and available to view by those named in 4.1 above. This is also password protected.
4.10. The system in the 6th form/library is similarly password protected and only premises staff and the Head and Deputy Head of the 6th form have passwords.
4.11. The system in the Student Support Centre is also password protected and only the premises staff, Director of Inclusion and BSWs have the password. This password is common to all who have access and it must not be passed on to any other person.
4.12. A disclosure log is kept to record any third parties who request recorded images.

5. Access to Live Images

5.1. Viewing of live images on monitors should usually be restricted to the operator and any other authorised person, i.e. CCTV operators, Leadership Team, KSCs, PALs, Director of Inclusion and BSWs as defined in point 4.1 above, where it is necessary for them to see it. However, as long as no students or unauthorised staff are present, such as may happen in the Leadership Team's offices, monitors may be left switched on.

5.2. Examples of when viewing of live images would be appropriate include:
- 5.2.1. To monitor congestion for health and safety purposes, unless the monitor displays a scene which is also in plain sight from the monitor location.
- 5.2.2. To monitor areas of the School premises that are out of sight or not frequently visited by staff.
- 5.2.3. When there is a suspicion that improper conduct may be carried out at a particular time.

5.3. In the Leadership Team's offices, the monitor must be switched off whenever students are present in the room.
5.4. The privacy of staff and students going about their normal legitimate business must be respected at all times.
5.5. See 4.7 to 4.10 above regarding password protected systems.

6. Storage of Recorded Material

6.1. All of the recorded images from all of our systems are stored digitally on the hard drives so there is no issue surrounding secure storage other than access to the images being limited to authorised persons.
6.2. Images remain on the hard drive as long as the memory allows. This is generally no longer than thirty days. Images are then automatically overwritten.

6.3. Images can be copied to 'archives' in case these need to be viewed at a later date, or burnt onto a disc or memory stick as evidence for the police. Archived images should be deleted after a three month period assuming they are no longer needed.

6.4. The Facilities Manager is responsible for reviewing the disclosure log and checking archived/stored images are deleted after this period.

7. Maintenance

The CCTV systems in School are maintained by DJ Byers Ltd. The date/time stamps on the systems are checked monthly by premises staff that they are correct and records are kept.

8. Subject Access Requests

8.1. When individuals make subject access requests, personal data will not be disclosed to that individual if the Police or other relevant enforcement agency confirm that this would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

8.2. Under the Data Protection Act 1998, access to images by persons captured on them, ("Subject Access") will be granted to parents/carers unless disclosure would prejudice criminal enquiries or criminal proceedings. The following procedures apply:

8.2.1. A written request must be submitted, including the following information: the date, the time (to within half an hour) and location of the incident to allow the images to be easily found. Vague requests involving long search times cannot be accepted.

8.2.2. When individual "subject access" requests are received, the School must establish whether disclosure of the images would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. It may be necessary to involve the police authorities in this process if determination of this is difficult. "Subject access" to view images will only be granted if disclosure is not deemed to prejudice the above. Subject access requested by a student will be carried out in accordance with Statutory Instrument 1437 of 2005 The Education (Pupil Information) (England) Regulations.

8.2.3. If all criteria are satisfactorily met, the School will undertake a search for any images and advise the individual by letter of the images which can be seen. The written response will be made within 15 School days of receiving the request if a student or within 40 consecutive days otherwise.

8.2.4. If the individual requires the viewing of images, then they must put their request in writing. If the identification of other individuals is inevitable through viewing the images, access to view would not normally be granted without the consent of those individuals unless it is reasonable in all the circumstances to do so without consent. Appropriate viewing arrangements will be made by School to view these extract images only, at a suitable location and time within a period of 40 consecutive days from receipt of the written request (or 15 School days if the individual in question is a student). The individual must provide satisfactory proof of identity.

8.2.5. If the individual subsequently requests a copy of the relevant images, this must be made in writing. Subject access requested by a student will be carried out in accordance with Statutory Instrument 1437 of 2005, "The Education (Pupil Information) (England) Regulations". Any copy CD-ROMs released to an individual may be retained by them.

8.2.6. School will also need to consider whether the consent of other third parties may be required for release of the images and whether any blurring or obscuring of images is required. If so, this must be carried out prior to disclosure.

8.2.7. Copyright remains with the School.

8.2.8. It should be noted that any initial request regarding capture of 8.2.1 above should be made in full within 7 days of the incident.

9. Responsibility for the Operation of the CCTV System

Guiseley School as Data Controller is responsible for the operation of the CCTV system. This policy is written by the Director of Administration and Finance and approved by the Governors' Resources committee. The operational responsibility is delegated to the Facilities Manager.

Appendix I

The Data Protection Act 1998: data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
   1.1. at least one of the conditions in Schedule 2 is met, and
   1.2. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix II

The guiding principles of the Surveillance Camera Code of Practice

System operators should adopt the following 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.