Policy on the use of CCTV on the site

Policy adapted from (if applicable):	N/A
Governing Body Sub-committee	
Name:	Site Committee
Date approved:	25 October 2018
Full Governing Body (if applicable)	
Date approved:	N/A

Context:
This policy is based on best practice guidance as detailed by the Information Commissioner's Office (ICO) publication "In the picture: A data protection code of practice for surveillance cameras and personal information" which is available to download from https://ico.org.uk/media/1542/cctv-code-of-practice.pdf and is referred to as ICO Code in this policy.

The policy also references the Data Protection Act 2018 (DPA) which may be accessed at www.legislation.gov.uk and the Surveillance Camera Code of Practice June 2013 (updated 28 October 2018), which is available at https://assets.publishingservice.gov.uk.

The ICO code has not been updated since General Data Protection Regulation (GDPR) came into force on 25 May 2018. However, the ICO Code states that differences between it and the new law are subtle and the information in the code is still considered to be useful.

Aims for use of CCTV cameras at the school:

- To prevent and detect crime, potentially enabling the school to take some action in relation to an individual(s), for example in handing the images over to the police.
- To protect the safety of Belper School and Sixth Form Centre users.
- To be in compliance with the DPA 2018 and the ICO Code in relation to responsible and lawful capture, processing, storage and eventual disposal of footage, including personal data.

Impact assessment

It is good practice under the ICO Code to consider the possible impact of using a CCTV system on organisation users. At Belper School and Sixth Form Centre we will:

- Use the images to monitor the presence of unauthorised people on the site, people who create disturbance, damage property, assault people, appear to break the law
- Will take responsibility for these images under the DPA 2018.
- Benefit legitimate users of the school via increased security, reduction of damage and a decrease of disruptive behaviour in public places in the school.
- Only use CCTV in circulation areas. It will not be used to monitor teaching.
- Only use images, not sound.
- Only install CCTV cameras after other methods of detection have been ruled out.
- Monitor CCTV use and seek the views of those who regularly use the site.
- Operate in accordance with the law operating at the time.
- Ensure that data use will be proportionate to the problem it is designed to deal with.

- Place notices adjacent to the cameras to inform people that a CCTV system is in operation, why it is in use and who manages the system (Data Controller) along with a contact number for enquiries.

Ensuring effective administration

1. The Head Teacher (HT) will have responsibility for control of the images and decisions on how they are used, and in his absence the Deputy Head Teacher (DHT) will take on this role.
2. Belper School and Sixth Form Centre is the Data Controller and has notified the Information Commissioner's Office (ICO) of this fact in respect of the CCTV images collected.
3. Only authorised employees of Belper School and Sixth Form Centre will process the images captured by the on-site CCTV.
4. The Head Teacher, or their representative will carry out proactive checks on a regular basis to ensure that these procedures are being complied with.
5. The Head Teacher, or their representative will be responsible for ensuring that the above procedures are followed.

Selecting and siting the cameras

The locations for the cameras have been selected in order to ensure that appropriate images are collected in accordance with the aims stated earlier. The system will not be used for the purpose of monitoring quality of teaching.

Equipment chosen

The equipment has been chosen in order to give clear, useful images of people on the site. These images will be stored for a limited period (usually 30 days) and then overwritten/deleted. No sound recording facility will be used on any CCTV cameras.

Storing and viewing the images

The images will be stored on the system and be accessible by the Network Manager or their nominated representative, the Head Teacher and their nominated representative(s). If an image is requested and the request is a valid one, the Network Manager or their nominated representative will download the required images for the user. If appropriate, the suggested fee will be levied (with regard to the legal maximum value).

The images will be accessible in the Caretakers' office so the Caretakers can view site security, especially when they are the only ones in the building. It will only be possible to see sufficient detail when close to the monitors so that people are aware of the CCTV use but not who is observed. Only the Network Manager or their nominated representative will be able to access these images as will the Head Teacher or their nominated representative.

A simple log of requests for data should be maintained in case of challenge. This should include date of request, name of person requesting personal information (images) and how the request was dealt with. This will be kept by the Network Manager or their nominated representative and stored in their area in the Library.

Disclosure

This will be in accordance with the DPA 2018 and the ICO Code and will take into account the rights of the individuals viewed on the images and any requests under the Freedom of Information Act (FOI).

To ensure that the CCTV system continues to comply with the DPA 2018 and the ICO Code of requirements in practice, if requested we will:

- direct those who make information/image requests to this policy;
- tell people how they can make a Subject Access Request, who it should be sent to and what information needs to be supplied with their request;
- give them a copy of the ICO Code or details of the (ICO) website; and
- tell them how to complain about either the operation of the system or failure to comply with the requirements of the ICO Code.

Staff training and awareness of procedures

Staff using the CCTV system or images will be trained to ensure they comply with the ICO Code. In particular, they will know:

- what the organisation's policy and procedures are for recording and retaining images
- how to handle the images securely
- what to do if they receive a request for images, for example, from the police
- how to recognise a subject access request and what to do if they receive one

The School Office Manager will also be aware of how to handle any requests/queries relating to CCTV use in school.

All images will be protected by sufficient security to ensure they do not fall into the wrong hands. This includes technical, organisational and physical security. For example, we will ensure that:

- sufficient safeguards are in place to protect wireless transmission systems from interception
- the ability to make copies of images is restricted to authorised and appropriate staff
- where copies of images are disclosed they are safely delivered to the intended recipient
- rooms where images are stored are secure
- relevant staff are trained in security procedures and they understand the sanctions that may be used against staff who misuse CCTV images
- all relevant staff are aware that they could be committing a criminal offence if they misuse CCTV images
- the process for deleting data is fit for purpose and adhered to

There will be an annual review of the use of CCTV in school, carried out by the Head Teacher or their nominated representative using a checklist. This procedure is described below in Appendix 1.

Guidance documentation is attached to this policy as a working appendix and will be reviewed regularly (annually), by the Head Teacher or their nominated representative. This is to ensure that school complies with the most recent relevant legislation and guidance in relation to use of CCTV on site.

Appendix 1: Annual Review Procedure

Checklist for users of limited CCTV systems monitoring premises

This CCTV system and the images produced by it are controlled by the Head Teacher of Belper School and Sixth Form Centre who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 2018).

Belper School and Sixth Form Centre governors have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of its users. It will not be used for other purposes. We conduct an annual review of our use of CCTV, carried out by the Head Teacher or their nominated representative.

	Checked (Date)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	1 October 2018	HT	1 October 2019
There is a named individual who is responsible for the operation of the system.	1 October 2018	HT	1 October 2019
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.	1 October 2018	DHT / Network Manager	1 October 2019
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	1 October 2018	DHT / Network Manager	1 October 2019
Cameras have been sited so that they provide clear images.	1 October 2018	DHT / Network Manager	1 October 2019
Cameras have been positioned to avoid capturing the images of persons not visiting the premises (or its immediate boundaries).	1 October 2018	DHT / Network Manager	1 October 2019

	Checked (Date)	By	Date of next review
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	1 October 2018	DHT	1 October 2019
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	1 October 2018	Network Manager	1 October 2019
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	1 October 2018	Network Manager	1 October 2019
Except for law enforcement bodies, images will not be provided to third parties.	1 October 2018	Network Manager	1 October 2019
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.	1 October 2018	HT	1 October 2019
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure, the Data Controller knows to seek advice from the Information Commissioner as soon as such a request is made.	1 October 2018	HT	1 October 2019
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	1 October 2018	DHT / Network Manager	1 October 2019

Appendix 2: The guiding principles of the Surveillance Camera Code of Practice

System operators should adopt the following 12 guiding principles:

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.

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.

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.

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

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.

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.

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.

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.

Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

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.

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.

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.