ST PHILIP HOWARD CATHOLIC HIGH SCHOOL

CCTV POLICY

Approved by governors: 2nd February 2016

Review date: February 2019

Introduction

The purpose of this document is to define St Philip Howard School's CCTV policy, to determine responsibilities, ensure we are operating a suitable CCTV system and to ensure that we are working within the law. The basic legal requirement of running a CCTV system is to comply with the Data Protection Act. As of 09-01-2012 the WSGFL website was pointing users to an out-date document dated 2000. This has since been replaced by the CCTV code of practice Revised edition 2008. A large amount of text from this later revision has been used to create this document. By completing this document and following recommendations in the CCTV Code of Practice we will:

- ensure that captured images of individuals comply with the DPA
- ensure that the images that are captured are usable
- reassure those persons whose images are being captured.

What this code covers

This code covers the use of CCTV and other systems which capture images of identifiable individuals or information relating to individuals for any of the following purposes:

- Seeing what an individual is doing, for example monitoring them in a shop or walking down the street.
- Potentially taking some action in relation to an individual, for example handing the images over to the police to investigate a crime.
- Using the images of an individual in some way that will affect their privacy, for example passing images on to a TV company.

Legal requirements for using CCTV

The use of CCTV is covered by:

- The Human Rights Act 1998
- The Data Protection Act 1998
- The Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012

By installing CCTV in the school, St Philip Howard:

- considers the wider human rights implications, in particular the right to respect for private and family life, one of the basic rights in the Human Rights Act.
- complies with the Data Protection Act – images captured on CCTV cameras are personal data and schools must comply with data protection principles. Individuals may view their images recorded on CCTV if they wish to do so.
- ensures it complies with the Information Commissioner’s Office (ICO) CCTV Code of Practice, available on the ICO website.
- has notified the Information Commissioner that CCTV cameras have been installed, stating the purposes for using the cameras.

Deciding whether to use CCTV or continue using CCTV

Using CCTV can be privacy intrusive, as it is capable of putting a lot of law-abiding people under surveillance and recording their movements as they go about their day to day activities. You should carefully consider whether to use it; the fact that it is possible, affordable or has public support should not be the primary motivating factor. You should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals **.**You should consider these matters objectively as part of an assessment of the scheme’s impact on people’s privacy.

CCTV Impact Assessment

What organisation will be using the CCTV images? Who will take legal responsibility under the Data Protection Act (DPA)?

St Philip Howard School controls its own CCTV system and no bodies outside of the school have access, or will be provided with, any images recorded. The only exception to the rule would be handing images over the police for the purpose of investigating a crime.

What is the organisation’s purpose for using CCTV? What are the problems it is meant to address?

The purpose of using CCTV is to protect staff, students, visitors and property from the actions of individuals. These actions may not necessarily be criminal offences but will have a negative impact on teaching, learning and employees' working environment. Being a secondary school with around 900 students covering a collection of buildings, monitoring behaviour using staff alone can be a challenge. CCTV images are recorded so that they can be used to establish who committed an offence. The CCTV recordings are used alongside traditional ways of investigating such as obtaining witness statements.

What are the benefits to be gained from its use?
To create a comfortable and safe learning and working environment.

Can CCTV technology realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
Yes, CCTV has proved many times to be of benefit in identifying individuals following an incident. St Philip Howard School is constantly working to improve student behaviour and the CCTV system has a positive impact on this.

Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?
Identifiable images of individuals are a necessity as this is the primary reason for having it.

Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?
The school has a new IP system where the cameras connect into the school network and are recorded onto servers.

What future demands may arise for wider use of images and how will you address these?
Additional cameras may be added if it is deemed necessary following incidents that cannot be resolved. As we install and manage our own system, the cost of expansion is kept to a minimum.

What are the views of those who will be under surveillance?
Although we have not surveyed people, we believe the following to be correct: Staff are aware that they are under surveillance and know that it is for their protection and not to monitor them working. Students feel protected having CCTV and we know that some park their bikes in front of cameras to keep them safe.

What could you do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed? No concerns have been raised but, if they were, we can assure them that images are only reviewed according to this policy and live feeds are kept away from general view.

<u>Ensuring effective administration</u>
Establishing a clear basis for the handling of any personal information is essential and the handling of images relating to individuals is no different. It is important to establish who has responsibility for the control of the images, for example, deciding what is to be recorded, how the images should be used and to whom they may be disclosed. The body which makes these decisions is called the data controller and is legally responsible for compliance with the Data Protection Act (DPA). **You will also need clear procedures to determine how you use the system in practice.**

Who has responsibility for control of the images and making decisions on how these can be used?
The Business Manager has responsibility for the control of the images and the decision as to how these can be used are made between them and the Head Teacher.

Have you identified and clearly defined specific purposes for the use of images, and have these been communicated to those who operate the system?
The purpose of using CCTV is to protect staff, students, visitors and property from the actions of individuals. These actions may not necessarily be criminal offences but will have a negative impact on teaching and learning and employees working environment.

This is a list of example incidences that would warrant reviewing CCTV images:

- Vandalism
- Intimidation
- Theft
- Missing Student
- Near miss incidents
- Accidents

This is a list of occurrences that would not justify the use of reviewing CCTV images:

- Staff or student punctuality
- Monitoring staff working

Some staff also have access to live feeds including operating pan tilt and zooms features of some cameras. These staff are listed in section 'Storing and Viewing the Images'.

Location of cameras

To judge the quality of images that will be necessary, you will need to take into account the purpose for which CCTV is used and the level of quality that will be necessary to achieve the purpose. The Home Office Scientific Development Branch recommends identifying the needs of a CCTV system by using four categories:

1. Monitoring: to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.

2. Detecting: to detect the presence of a person in the image, without needing to see their face.

3. Recognising: to recognise somebody you know, or determine that somebody is not known to you.

4. Identifying: to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

For St Philip Howard, categories 1 and 2 do not apply. Category 3 in almost all cases would be the reason for having cameras. Number 4 would only apply in rare cases.

Using the equipment

It is important that a CCTV system produces images that are of a suitable quality for the purpose for which the system was installed. If identification is necessary, then poor quality images which do not help to identify individuals may undermine the purpose for installing the system.
Do the recorded pictures and prints as well as the live screens produce good clear pictures? This is important to ensure that there has not been an unacceptable loss of detail during the recording process.

The new camera system installed during 2012 records images that are entirely suitable for the needs of the school

Have you considered the compression settings for recording material? In a digital system, a high level of compression will result in poorer picture quality on playback.

Compression has been kept to a minimum.

Have you set up the recording medium in such a way that images cannot be inadvertently corrupted?
Yes, only the IT Manager has admin access to the system.

Is there a regular check that the date and time stamp recorded on the images is accurate?
The systems have been set up to get the time from the school Curriculum server. This is monitored on a regular basis and changed if needed.

If automatic facial recognition technology is being used, are the cameras placed so that facial images are clearly captured? Are the results of any match checked by people before any action is taken? N/A: No facial recognition used.

Has a regular maintenance regime been set up to ensure that the system continues to produce high quality images? Yes via the company who installed our system – Prime Digital.

If a wireless transmission system is used, are sufficient safeguards in place to protect it from being intercepted? Yes, protected by firewalls.

CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified. You should choose a system without this facility if possible. If your system comes equipped with a sound recording facility then you should turn this off or disable it in some other way. St Philip Howard does not use CCTV to record any conversations and all these features have been turned off on the equipment.

Storing and viewing the images

Recorded material should 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. To do this you need to carefully choose the medium on which the images are stored, and then ensure that access is restricted. You may wish to keep a record of how the images are handled if they are likely to be used as evidence in court. Finally, once there is no reason to retain the recorded images, they should be deleted. Exactly when you decide to do this will depend on the purpose for using CCTV. **It is important that your images can be used by appropriate law enforcement agencies (The School) if this is envisaged. If they cannot, this may undermine the purpose for undertaking CCTV surveillance.**

How easy is it to take copies of a recording off your system when asked for by a law enforcement agency? Can this be done without interrupting the operation of the system? The enforcement agency is the school itself. The IP systems are quite straight forward to take copies of images. Data can be taken from the system without interrupting recording.

Will they find your recorded images straightforward to use?
Any data removed will be in a standard computer video file format or standard still image format.

What will you do when recorded material needs to be taken away for further examination?
If any data goes off site, there is a procedure to record what has been provided including the incident details, a crime number if appropriate and who it has been given to. A copy is also kept by the school.

Viewing of live images on monitors should usually be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location. Example: Customers in a bank can see themselves on a monitor screen. This is acceptable as they cannot see anything on the screen which they could not see by looking around them. The only customers who can see the monitor are those who are also shown on it. **Example:** Monitors in a hotel reception area show guests in the corridors and lifts, i.e. out of sight of the reception area. They should be turned so that they are only visible to staff, and members of the public should not be allowed access to the area where staff can view them. **St Philip Howard has the following live feeds:** Reception, Site & Premises Manager, 2 x Assistant Site and Premises Officers, Attendance Secretary, Business Manager, IT Manager, from computers where the screen face away from other staff and students.

Recorded images should also be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to authorised persons.

Are your monitors correctly sited taking into account the images that are displayed?
Yes, within either the Site Office, IT Office or Business Manager's office, all of which are secure and not visible to passing pupils, visitors or unauthorised staff.

Is your monitor viewing area appropriate and secure?
Yes, not visible to pupils or visitors.

Where necessary is access limited to authorised people?
The following staff have access to live feeds and to recorded data and are regarded as CCTV Operators:-

- Jill Alcorn –Business Manager
- Richard Steer – Assistant Network Manager
- Mandy Gavin – Assistant Network Manager
- Dave Bliss – Site and Premises Manager
- Danny Murray – Assistant Site and Premises Officer
- Kevin Dart – Lettings Officer

The above staff have access to these feeds from their own offices as no one can see their screens.

- Sally Powney– Attendance Officer, Caroline North & Abigail Vinter – Receptionists and Kevin Dart – Lettings Officer have been given permission to view CCTV but not to record or review data on their computers.