Our Lady's Catholic College

Local Policy

Control of CCTV / Data protection

Completed by Anne Eaves – CCTV System Manager

Issue date – 11 April 2017
Review date – 9 April 2017

Contents

23. Destruction of data

24. Audit process

1 - Purpose

The purpose of this policy is to ensure that the college is complying with the Regulation of Investigatory Powers Act 2000 (RIPA) and the Data Protection Act 1998.

This policy has been created to ensure compliance with the Information commissioner's office CCTV code of practice 2008. Compliance with the code of practice helps to ensure that good practice standards are adopted by those who operate CCTV. If OLCC follows the code's provisions this not only helps OLCC remain within the law but fosters public confidence by demonstrating that OLCC takes its responsibilities seriously.

Most CCTV is directed at viewing and/or recording the activities of individuals. This means that most uses of CCTV by organisations or businesses will be covered by the Data Protection Act (DPA) and the provisions of this code, regardless of the size of the system. The DPA applies to images captured by CCTV. The code does not cover the use of dummy or non-operational cameras. To aid OLCC achieve compliance with the code an impact assessment has been completed using a range of questions taken directly from the code.

2 – Impact assessment

To ensure that OLCC is complying with the code of practice a separate impact assessment has been completed and is available from the school manager on request.

Question 1
What organisation will be using the CCTV images? Who will take legal responsibility under the Data Protection Act (DPA)?

Answer
Our Lady's Catholic College is a Catholic Voluntary Aided school in the diocese of Lancaster. The school is local authority maintained under the umbrella of Lancashire County Council. The school budget and admission criteria are set by the board of governors. CCTV images will be used within the school as part of a wider strategy to minimise the risk to students, staff and property. The board of Governors will take legal responsibility for the protection of school data under the data protection act.

Question 2
What is the organisation's purpose for using CCTV? What are the problems it is meant to address?

Answer
The purpose of using CCTV within OLCC is to ensure the following risks are minimised:

- Bullying and/or physical abuse or any other 'harm' to any member of our school community
- Damage to or theft of property
- To help support or refute allegations against any member of our school community that are detrimental to the health, safety, wellbeing or educational opportunities (including the 'right to learn') of any other member(s) of our school community
- Intrusions
- Truancy
- Malicious use of fire alarms
- To help enforce student rules generally

A typical example of how CCTV has aided the school to minimise the risks to the health and safety of students, staff, contractors and property is the following incident that took place in March 2012 – A school bin was set alight by a student putting the safety of the school and its occupants at risk. The fire was extinguished and an investigation took place. CCTV provided valuable evidence in identifying the suspect who started the fire.

Another example is truancy. Students who avoid lessons leave the site using weak points in the perimeter fencing. CCTV is used to identify the students and this subsequently assists in deciding what action to take to reduce truancy.

CCTV is a visible deterrent. Students are fully aware of the cameras and they are a valuable asset in the strategy to create a community driven school where respect for each other and for the environment is paramount.

CCTV has also been used in the past to refute false claims by employees of injuries at work and evidence in cases of serious breaches of the Staff Code of Conduct.

CCTV has not and would not be used as a proactive 'monitor' of any individual member of the community's actions unless there were already serious concerns raised with regard to that individual's actions and CCTV could help allay or confirm those concerns.

Question 3
What are the benefits to be gained from its use?

Answer
CCTV supports the Headteacher's vision of a well controlled learning environment. Through correct use of CCTV, instances of poor behaviour are captured and challenged again and again by staff. The aim is to improve student behaviour and create a safe, secure well organised school.

Question 4
Can CCTV technology realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?

Answer
CCTV is the only realistic method of capturing images that can be used as evidence. The school is significant in size with student access spread throughout the buildings and grounds. Staff do monitor student behaviour as much as possible but the scale of the site makes it unrealistic for effective people-based monitoring and supervision.

Question 5
Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?

Answer
The school requires technology capable of identifying individuals as part of behavioural improvement plans. Incidents involving poor behaviour relate directly to students. In order to challenge this behaviour identification of students and members of staff is required. No other technology can deliver this requirement.

Question 6
Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?

Answer
Yes, CCTV has already proved valuable in achieving its aims and has assisted in reducing incidents of poor behaviour. Due to the success of the system it is highly likely that the system will remain suitable for the foreseeable future. A review of specific cameras will take place in order to try and reduce unnecessary monitoring.

Question 7
What future demands may arise for wider use of images and how will you address these?

Answer
There are no expected demands for the wider use of images from the CCTV system. Should demands arise i.e. subject access requests or evidence based usage then local policy will be followed to ensure compliance with the Data Protection Act.

Question 8
What are the views of those who will be under surveillance?

Answer
Students, staff and parents have welcomed the results from our installation. The benefits of challenging poor behaviour and detecting incidents of truancy are helping the school enhance its reputation as a market leader, this in turn helps to create and maintain a learning environment.

Question 9
What could you do to minimise intrusion for those that may be monitored, particularly if

specific concerns have been expressed?

Answer
No specific concerns have been raised, however as part of the annual review process all areas that are covered by CCTV will be evaluated for effectiveness. Coverage within toilet facilities has been limited to entry and wash hand basin areas. This installation has reduced the amount of reported incidents of smoking and damage to property.

3 - The Human Rights Act

OLCC operates the CCTV system on behalf of Lancashire County Council. OLCC therefore has a responsibility to consider wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life). Questions include:

Question 1
Is the proposed system established on a proper legal basis and operated in accordance with the law?

Answer
The system has been designed and installed by an approved company and in accordance with regulations. The system is operated with the support of a local policy based on the Information commissioner's office CCTV code of practice 2008.

Question 2
Is it necessary to address a pressing need, such as public safety, crime prevention or national security?

Answer
Yes, the school has a number of behavioural based issues that require support from technology. The issues relate to public safety and the prevention of crime.

Question 3
Is it justified in the circumstances?

Answer
Yes, the school has a number of issues that require intervention with the aid of technology. Due to the limited but wide ranging categories of poor behaviour the system is justified.

Question 4
Is it proportionate to the problem that it is designed to deal with?

Answer
Yes, CCTV is an aid only and will provide valuable evidence to support the schools aims. Most cameras are static and deemed a proportionate response to the wide ranging issues the school suffers from.

4 – Overview of CCTV within OLCC

The site has been surveyed by the site manager and installation contractor to ensure that an appropriate number and type of cameras are installed in suitable locations. The system records images 24hrs per day. This is due to the wide ranging security issues the school suffers from. The site covers an extensive area and is surrounded by populated areas. There is a high likelihood of damage to property and theft.

The decision to site cameras with toilet wash hand basin areas has been based on consistent poor behaviour within toilet areas. Poor behaviour ranges from extensive damage to property, smoking and bullying. Cameras are positioned in wash hand basin areas only to protect privacy. CCTV signage is positioned on the door to enter the toilet area.

No cameras within OLCC are equipped with an audio recording facility.

The college has a total of 45 CCTV cameras positioned as follows:

25 located within the site buildings
20 located within the grounds of the building

The School Manager has overall delegated accountability and control of the following aspects of CCTV within the site:

- The positioning of the cameras during any new installations or as part of any refurbishment.
- Maintaining a list of authorised users of the CCTV system
- Allocation of passwords for authorised users of the CCTV system
- Allocation of security keys to access the CCTV room
- Data protection

The site manager maintains a site plan of the specific location of each camera.

5 - Register of CCTV cameras including location and type

The college has a total of 45 cameras based in interior and exterior locations. The specific locations of the cameras are as follows:

BSU - Static
Sixth form first floor - Static
Sixth form first floor study room - Static
Sixth form phase 1 entrance - Static
Sixth form ground floor common room - Static
Sixth form ground floor common room - Static
Main building balcony - Static

3 Storey corridor to gym - Static
Gym entrances - Static
2 Storey boys toilets - Static
3 Storey Girls toilets - Static
3 Storey Boys toilets – Static
3 Storey ground floor entrance yard next to staff room - Static
3 Storey first floor oratory - Static
3 Storey second floor exam office - Static
3 Storey ground floor corridor – Static
3 Storey corridor ground floor - Static
3 Storey ground floor outside English office - Static
2 Storey ground floor corridor – Static
2 Storey ground floor corridor - Static
2 Storey ground floor corridor - Static
Sixth form main entrance - Static
Main building front entrance - Static
Main building outside site supervisors office – Static
Main building – Assembly hall - Tilt/Pan/Zoom

External cameras

2 Storey - Path from MML to side entrance of 2 storey – Static
3 Storey - Corner coverage - Static
Drama studio – Side of studio - Static
Courtyard - Static
2 Storey – Overlooking boiler house - Static
Sixth form – Rear of building - Static
MML – Overlooking fenced garden - Static
2 Storey – Overlooking MML fenced garden area - Static
MML – Front of library - Static
Sixth form – Overlooking rear of building - Static
3 Storey - Overlooking sports field - Tilt/Pan/Zoom
Technology – Overlooking technology and drama area - Tilt/Pan/Zoom
Sixth form – Overlooking courtyard - Tilt/Pan/Zoom
Sixth form – Overlooking external areas of building - Tilt/Pan/Zoom
Gym corridor – Overlooking courtyard - Tilt/Pan/Zoom
Kitchen – Overlooking car park - Tilt/Pan/Zoom
MML – Overlooking library car park - Static
2 Storey – Overlooking bike store - Static
2 Storey – Overlooking main entrance - Static
MML – Overlooking rear of MML - Static

Summary of CCTV

Location of cameras
Internal Cameras = 25

External cameras = 20

Type of cameras
Static = 38
Pan/Tilt/Zoom = 7

6 - Administration

- Mrs Helen Seddon - Head Teacher and School 'Data Controller'
- Mrs Anne Eaves - Business Manager and 'CCTV System Manager'
- Mr Neil Storey - Site Manager, Mr Wal Jackowski & Mr Ben Storey - Site Supervisors - Operators and will playback images as part of any investigations. May also provide recorded data to the Head teacher or Business Manager as instructed.

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). The schools governing body is the Data Controller for OLCC for the purpose of compliance with the Data Protection Act.

There are a number of responsibilities and obligations that the data controller has to comply with. The content of this local policy has been approved by the governing body and will ensure all aspects of the use of CCTV at OLCC is compliant with the code of practice and Data Protection Act.

7 - Signage

The college has signage in camera installed areas stating that CCTV monitoring is in operation. New installation or refurbishment must include new signage to ensure that the students, staff and members of the public are aware of the presence of CCTV.

8 - Security of and access to the CCTV room

The CCTV room is secured with a 5 lever lock. Keys to access the room are restricted to the site manager and site supervisors. No other person is authorised to enter the room without the permission of one of the key holders. The CCTV room contains a list of authorised users for reference.

9 - Control of static CCTV cameras

The site does not use CCTV operators to monitor the site. CCTV is captured to hard drives and data can be viewed and used for evidential purposes if required. CCTV is an aid to minimise the risk to the safety and security of students, staff, contractors and members of the public. The college has a significant number of fixed static cameras. The cameras have been

positioned to ensure that the coverage of the site is as wide as possible and able to capture a view of a populated area and not focused on any individual. Static cameras can only be moved by the approved contractor and with the permission of the school manager.

10 - Control of Tilt, Pan and Zoom CCTV cameras

The college has a minimum amount of these cameras. They are located in areas where coverage is of a wide expansive area such as the sports field. Authorised operators will operate the Tilt, Pan and Zoom to capture a general view of the site at unpredictable times to maintain safety and security of the site. Operators will not target any specific individual or group of people unless in response to an unplanned and spontaneous event i.e. a breach of site rules, disorder or for the prevention or detection of a crime. In the event of a spontaneous event the operator will create a written record within the incident log in the CCTV office and report this to the site manager. At no time must the operator target an individual or group of people other than for a spontaneous event.

11 - Accessing the CCTV control panel (Playback and Hard drive access)

Access to the CCTV control panel is restricted to the Headteacher. school manager, site manager and site supervisors. Access is password protected to each individual user.

12 - Control of playback of stored data

Teaching staff have been provided with delegated authority to view recorded CCTV data when the need arises i.e. in connection with an incident that may reveal a breach of college rules or a child protection issue etc. Only footage related to the incident must be viewed. The authorised people who can access the control panel will facilitate the viewing.

13 - Disclosure

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet.

Images can be released to the media for identification purposes; this should not generally be done by anyone other than a law enforcement agency.

NOTE: Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

Any other requests for images should be approached with care, as a wide disclosure of these

may be unfair to the individuals concerned. In some limited circumstances it may be appropriate to release images to a third party, where their needs outweigh those of the individuals whose images are recorded. In all cases the school manager must be consulted prior to the release of any images.

Example: A member of the public requests CCTV footage of a car park, which shows their car being damaged. They say they need it so that they or their insurance company can take legal action. You should consider whether their request is genuine and whether there is any risk to the safety of other people involved.

Judgements about disclosure will only be made by the school manager.

The school manager has the discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. If the school manager authorises disclosure of an image to another body, such as the police, then they become the data controller for their copy of that image. It is their responsibility to comply with the Data Protection Act (DPA) in relation to any further disclosures.
The method of disclosing images should be secure to ensure they are only seen by the intended recipient.

14 - Subject access requests

Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. This must be provided within 40 calendar days of receiving a request. The school manager may charge a fee of up to £10 (this is the current statutory maximum set by Parliament).

Those who request access must provide the school manager with details which allow you to identify them as the subject of the images and also to locate the images on the CCTV system.

The school manager will consider the following on a case by case basis:

- Whether an individual will need to supply a photograph of themselves or a description of what they were wearing at the time they believe they were caught on the system, to aid identification?
- Whether details of the date, time and location are required?
- How will you provide an individual with copies of the images?
- If images of third parties are also shown with the images of the person who has made the access request, you must consider whether you need to obscure the images of third parties.
- If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured.

In many cases, images can be disclosed as there will not be such intrusion.

Example: A public space CCTV camera records people walking down the street and

going about their ordinary business. Where nothing untoward has occurred, this can be released without editing out third party images.
Example: Images show the individual who has made the request with a group of friends, waving at a camera in the town centre. There is little expectation of privacy and the person making the request already knows their friends were there. It is likely to be fair to release the image to the requester without editing out the faces of their friends.

Example: Images show a waiting room in a doctor's surgery. Individuals have a high expectation of privacy and confidentiality. Images of third parties should be redacted (blurred or removed) before release.

Where the school manager decides that third parties should not be identifiable, then arrangements will be made to disguise or blur the images in question. It may be necessary to contract this work out to another organisation. Where this occurs, the school manager will need to have a written contract with the processor which specifies exactly how the information is to be used and provides the school manager with explicit security guarantees.

15 - Freedom of information requests

As a public authority OLCC may receive requests under the Freedom of Information Act 2000 (FOIA) or Freedom of Information (Scotland) Act 2002 (FOISA).

The school manager is responsible for responding to freedom of information requests, and understands the authority's responsibilities. They must respond within 20 working days from receipt of the request. Section 40 of the FOIA and section 38 of the FOISA contain a two-part exemption relating to information about individuals. If the school manager receives a request for CCTV footage, they will consider the following:

- Are the images those of the requester? If so then that information is exempt from the FOIA/FOISA. Instead this request should be treated as a data protection subject access request as explained in the subject access request section.

- Are the images of other people? These can be disclosed only if disclosing the information in question does not breach the data protection principles. In practical terms, if individuals are capable of being identified from the relevant CCTV images, then it is personal information about the individual concerned. It is unlikely that this information can be disclosed in response to an FOI request as the requester could potentially use the images for any purpose and the individual concerned is unlikely to expect this. This may therefore be unfair processing in contravention of the Data Protection Act (DPA).

This is not an exhaustive guide to handling FOI requests.

Note: Even where footage is exempt from FOIA/FOISA it may be lawful to provide it on a

case-by-case basis without breaching the DPA, where the reason for the request is taken into account. See section titled (using the images) for advice on requests for disclosure.

16 - Other responsibilities

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 distress (s10 DPA) and one to prevent automated decision-taking in relation to the individual (s12 DPA). Experience has shown that the operators of CCTV systems are highly unlikely to receive such requests. If you do, guidance on these rights is available from the Information Commissioner's Office. Further information about the FOIA can be found on ICO's website: www.ico.gov.uk including specific guidance about section 40 (FOI Awareness Guidance No1).

17 - Authority to transfer data from hard drive to DVD

CCTV data is stored on static hard drives located within a locked room. The data can only be accessed by an authorised operator. Transfer of data to DVD must be kept to a minimum to reduce the risk of data loss. There are a number of reasons why data should be transferred to DVD i.e. Internal Investigations, Criminal investigations, subject access requests, litigation and for storage of evidence.

Should data be required to be transferred then the authority for transfer must be given from the Head Teacher or School manager prior to asking an authorised operator to complete the transfer. Under no circumstances can data be transferred without the authority of one of these 2 people. The procedure for transferring data from the CCTV hard drives to a DVD is as follows;

1. Data from CCTV transferred to a USB pen drive
2. Data from USB pen drive transferred to PC with DVD recording facility
3. DVD created from PC
4. USB pen drive formatted to erase data
5. Data on PC deleted
6. Created DVD logged in evidence file to account for chain of evidence
7. DVD stored in safe or handed to authorised person

18 - Register of data transfer

Details of the data transfer will be recorded as follows:

- Within the DVD data transfer register
- On the cover of the data disc

The register will display the following information:

- The date and time of copying

- The name of the person who has granted permission for the transfer to proceed
- The reason for the transfer
- The name of the person taking receipt of a copy of the data i.e. investigator, or police etc.

The completed disc will be physically handed to the person who is authorised to take receipt of the disc. At no time must a disc be placed in the postal system.

19 - Control of copied data

If there is a specific reason for a copy of the data to be handed over to a third party and they have received the permission from the school manager the authorised operator will create the disc. If permission has been granted the copy should be physically handed over to the third party and a record of the following information recorded within the DVD data transfer register:

- The date and time
- The name of the person who has granted permission for the handover to proceed
- The reason for the handover
- The name of the person taking receipt of the working copy disc i.e. investigator, or police etc.

20 - Control of Data in the possession of a member of staff

If a member of staff has been given the necessary permission to obtain a copy of data they should retain the data when not in use within an immovable safe that is secured within the site. The person who has taken receipt of the data becomes the data controller and they are responsible for the security of the data whilst it is in their possession.

At no time must the data be taken off the site without the permission of the school manager. The data must not be handed over to anyone else or viewed without the permission of the Headteacher or School manager, if permission is granted then the site manager must be informed and the data register will be updated to reflect the last handover.

If the copy of the data is no longer required then it must be returned to the site manager who will arrange for the safe storage of the data.

21 - Control of Data in the possession of a third party

If a third party has been granted permission for a copy of the data i.e. the Police, the third party becomes the data controller. They are responsible for the security of the data and have no obligation to return the data to the site. It is very important that any request from a third party for a copy of CCTV data is scrutinised and handled in accordance with data protection.

22 - Storage of data

Copies of data via DVD will be stored within an immovable safe to ensure the security of the data is maintained at all times. Only the authorised operators i.e. school manager, site manager, site supervisor can access the stored data.

23 - Destruction of data

The school manager will determine the time limit to retain data discs in accordance with principle 5 of the data protection act. Data discs that are no longer required will be destroyed with the use of a disc shredder. Third parties who are in possession of a data disc will be contacted by the school manager to enquire if the data is no longer required. If the data is not required a written request for destruction should be made to the third party.

Hard drives that are no longer required will be stored in the site safe until the school manager determines what time period they should be retained for. The head of IT will arrange for an approved contractor to destroy the hard drives and provide a transfer note with details to the school manager of the destruction.

24 - Audit process

The school manager will complete ad-hoc checks of the system and report the finding to the Head teacher to ensure compliance with this policy.