Cardinal Heenan Catholic High School

CCTV Policy

Key staff:	J Asquith
Key governor:	
Last reviewed:	January 19
Approved by Governing Body: Date:	*A Tremarco* January 2020
Due for renewal:	January 2021

CONTENTS

CONTENTS / INDEX **PAGE**

Policy Statement

Cardinal Heenan Catholic High School sets out to comply with the Data Protection Act 2018, General Data Protection Regulation (GDPR) and ICO CCTV Code of Practice 2008 where it uses CCTV systems. This policy statement and the following guidance must be complied with at all times on Cardinal Heenan Catholic High School premises.

1. Cardinal Heenan Catholic High School must ensure that there is reasonable justification before CCTV is used.

2. Cardinal Heenan Catholic High School has taken steps to ensure that the CCTV, when viewing perimeter fencing, does not invade neighbours' privacy.

3. A designated person will have legal responsibility of the scheme (Data Protection Officer).

4. The intended use of the CCTV will be documented and the system will not be used for anything other than this.

5. The administration of the system, will include:

   - Ensuring notification on an annual basis.
   - Ensuring the scheme is in accordance with the notification.
   - Procedures for handling images.
   - Record keeping of access requests, use of images procedures and pro-active monitoring of the scheme to ensure compliance.
   - Control of recorded material.

6. The CCTV system is sited only to achieve what is documented in the scheme.

7. Permanent or movable cameras will not be used to view areas that are not of interest and not intended to be the subject of the scheme. There are areas where there is an expectation of heightened privacy and CCTV may only be used in very extreme cases and will not be undertaken without correct notification to the headteacher / school business manager at the school.

8. The equipment will be maintained to give reliable quality.

9. No sound recording technology will be used.

10. Material will not be stored for longer than is necessary and will be deleted as soon as possible

11. Images will be viewed in a secure/restricted area with access only to authorised persons.

12. Images will not normally be released to third parties. Police may legitimately request images. (Section 35 PDA allows for disclosure of data in respect of court and other proceedings).

13. Individuals who are recorded may request access to the images specific to them.

14. There will be adequate signage to let people know that surveillance is taking place. Where cameras are discreet, the notices will be more prominent.

15. The CCTV systems will not be used to systematically monitor a specific person.

16. The scheme will be reviewed regularly by the governing body.

All staff that use the CCTV will be trained and aware of this policy statement, the Data Protection Act 1998, the CCTV Code of Practice 2008 and the guidance developed by Cardinal Heenan Catholic High School

Signed……

Position…….

Introduction

1. Closed Circuit Television (CCTV) is now a well-established and accepted practice in our lives. It is widely used in towns, shopping areas, hotels, schools and on the road networks. CCTV is generally supported by the public, but it does intrude into people's lives as they carry out their daily activities. This therefore means that responsible use, under guidelines, must be maintained to ensure that this 'intrusion' is legitimately carried out.

2. A code of practice for CCTV was issued in 2000 by the Information Commissioners Office (ICO) and this has since been replaced by the 2008 revised edition. The 2008 edition strengthens the 2000 code by taking into account the advancement of technology. The code is available at:

3. The code has been developed to ensure operators of CCTV systems follow good practice guidelines and comply with the law, in particular the Data Protection Act 1998 (DPA). Information about individuals (including images) that is held by any organisation, including local authorities, is covered by the DPA. The DPA has a number of **principles**, which are legally enforceable and are briefly included within this document (refer to Liverpool City Council's Data Protection policy for full details).

What is covered by the Code of Practice?

4. The 2008 code of practice covers CCTV systems which capture images of identifiable individuals, or information relating to individuals.

5. There are certain cases where the DPA is not applicable. These include:

   - Householders who have CCTV for domestic use, e.g. to protect their properties.

   - Images captured by individuals for personal (domestic) use on digital camera, mobile phones or camcorders.

6. Please note that any directed surveillance for law enforcement purposes is covered by the Regulation of Investigatory Powers Act (RIPA) 2000 and may require authorisation (contact Legal Services for further details).

When to use CCTV

7. Prior to installing a CCTV system, which must comply with the DPA, you must consider whether it is necessary or whether there is an alternative solution. For example, if the CCTV is purely for security, improved fencing and lighting may be a better option and won't require compliance with the DPA.

8. The code requires organisations to conduct an assessment before installation, to establish the following:

   - Who is legally responsible for the system?

   - What will the system be used for and how will it benefit the organisation?

- Can other, less intrusive, alternatives be used, such as lighting or improved fencing?

- Does the scheme capture images of identifiable individuals?

9. The Information Commissioner's Office states that if you are establishing a large system or considering a use of CCTV which could give rise to significant privacy concerns you may wish to consider using its Data Protection Impact Assessment.

   https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

Guidance for Schools

10. CCTV is an established part of everyday life and a proven tool in the fight against bullying, vandalism, graffiti and theft. One of the most rapidly expanding areas of use is in the education sector. CCTV is often used for surveillance in schools to prevent crime. Often, cameras are positioned to protect school premises and the general fabric of the building which helps to deter unwanted intruders from entering the schools perimeter. This has been particularly useful during school closures or holidays. Recently, there has been an increase in the use of CCTV not only for the purpose of protecting the school but for the intention of monitoring pupils and staff for the purposes of health and safety. This emerging trend has raised serious concerns within education circles claiming that this type of surveillance is an infringement of privacy laws.

11. Careful consideration should always be given to whether to use CCTV in the first instance; the fact that it is possible, affordable or has public support should not be the primary motivating factor. Schools should take into account what benefits can be gained and whether alternative solutions exist, and what effect it may have on individuals.

12. It would be strongly advisable to consult with staff, Governors, pupils and parents before installing any kind of CCTV system. It is recommended that the data controlling officer conducts a full consultation with all relevant parties. The consultation should include an explanation of all the purposes for which the CCTV cameras are being, or have been, installed and confirmation that they comply with the law as described in this policy.

13. Below is a list of common reasons why schools may consider installing CCTV:

    - Improving safety for staff
    - Tackle bullying
    - Reduce damage by vandalism
    - Tackle graffiti
    - Reduce theft
    - Deter the arsonist
    - Prevent pupils carrying knives into school
    - Eliminate boisterous activity in classrooms and general bad behaviour
    - Prevent cheating in exams
    - Improve safety and security during periods of extracurricular activity
    - Protect the school and staff against malicious or ill-conceived compensation claims.

14. If CCTV is to be used, privacy must be safeguarded by ensuring that cameras are not directed at cubicles or urinals and ideally are sited outside main entrances / exits to toilets and washrooms. There have been many protests recently against the use of toilet block surveillance by both pupils and parents claiming that it is 'a step too far'. However, some individuals have claimed that there should be nothing to fear as long as pupils and staff conduct themselves according to school policy and house rules regarding behaviour.

15. CCTV should always be used proportionally and with caution and where there are justifiable concerns that make it necessary for cameras to be fitted. Circumstances might be when persistent thefts have occurred or if it is suspected that persistent bullying is taking place. However, even in those circumstances, this should be time limited, proportional and all staff and pupils should be fully informed of the reason/s why the cameras are present.

16. Below is a list of situations where CCTV should not be used:

- Cameras should not be fitted in staff rooms unless required for security reasons when the rooms are not occupied. In this case, it should only be switched on during those periods.

- Schools must be careful not to include captured images of surrounding properties and gardens, as this will contravene data protection regulations.

- In no circumstances should CCTV be placed in such a way that it could capture images of pupils changing.

17. Further advice and guidance for schools is available from Liverpool City Council's Data Protection Officer (DPO).

Legal Issues

18. This policy has due regard to the legislation and statutory guidance, including, but not limited to the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 2004
- The Equality Act 2010

19. This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'.

20. This policy operates in conjunction with the following school policies:

- Photography and Videos at School Policy
- GDPR Data Protection Policy

Compliance with the Human Rights Act

21. The Human Rights Act 1998 (HRA) gives individuals the right to respect for their private and family life, home and correspondence. Public authorities may not interfere with this right except where necessary and in accordance with the law, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In practice, this means that authorities can use CCTV but only after they have risk assessed the impact on others privacy, whether the scheme is necessary, and for what purpose the images will be used.

Compliance with the Data Protection Act

21. **Principle 1** of the DPA requires that personal data is processed fairly and lawfully, i.e. that individuals are aware that images are being captured on CCTV, and of how that information will be used.

22. This means that signs, which are clearly visible and legible, should be displayed so that the public are aware they are entering an area where CCTV is in use. The signs should display details of the organisation responsible for the scheme, their contact details and the purpose of the CCTV system.

23. To ensure that images are only captured for the intended purpose of the scheme, the location of cameras must be carefully considered.

- The CCTV should be used only to monitor the intended spaces.
- Owners and residents of domestic premises should be consulted if domestic premises border the intended area to be viewed.
- Those operating the system must be fully trained, must be aware of what the scheme should be used for, and must only use the cameras and images for that purpose.

24. **Principle 2** requires that personal data be obtained for a specific purpose. Therefore if you install CCTV for security purposes you would normally only use that information for that purpose and wouldn't use it, for example, for staff monitoring.

25. Principle 2 also requires an organisation to notify to the Information Commissioner the purposes they process data for. If you use a CCTV system which will obtain personal information (i.e. images of individuals), you must ensure that your notification to the ICO includes this. Please note that all Council departments will be covered by the Councils notification which includes the purpose of processing information for crime prevention, safety and security. Other organisations (such as schools), which are a separate legal entity, will not be covered by the Council notification and must ensure they have their own notification in place.

26. **Principle 3** of the DPA requires that personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. This means that you should only collect the amount of data you need for the purpose the CCTV system has been installed for. You should collect no extra information and you need to ensure that the images will be adequate for their intended use.

27. **Principle 4** of the DPA requires that information should be accurate and up to date. The quality of images must be maintained to ensure that data within them is accurate and adequate for the intended purpose. In order to achieve this:

- Equipment should be maintained, serviced and cleaned regularly to ensure it performs correctly and a maintenance log should be kept.
- Footage should be of good quality and should be updated when necessary.
- If the system records location of camera, date, time etc. these should be accurate.
- Cameras should be protected from vandalism or tampering.

28. **Principle 5** of the DPA requires that information is held no longer than necessary for the intended purpose. Once a retention period has expired, images must be erased.

29. **Principle 6** of the DPA gives individuals certain rights under the Act. Section 7 of the DPA gives individuals the right of access to any personal data an organisation holds about them. This includes CCTV images and they have a right to view those images or request a copy.

30. A standard subject access request form is available upon request from the school.

31. If individuals request CCTV images they should be asked to complete the form (on Guidance Note 3 on the link above) and provide any necessary identification (see form for further details).

32. **Principle 7** of the DPA requires that information is held securely. Access to images, monitors and equipment should be by authorised staff only and copies of images should be stored securely.

Disclosure of CCTV Images

33. Access to, and the disclosure of, CCTV images and the disclosure of images to third parties should be restricted and carefully controlled to ensure the rights of individuals are protected.

34. All access should be documented (whether information is provided or refused), and disclosures must be limited to those allowed by law to Liverpool City Council.

35. **Principle 8** of the DPA requires that information is not transferred outside the European Economic Area unless certain criteria are met. Take advice from Legal Services if any images are requested from any organisation outside of this area.

Compliance

36. To ensure compliance with the above requirements, please complete the user checklist (Appendix A) and CCTV Policy document (Appendix B) and forward to the Data Protection Officer, Legal Services

Advice

37. For further advice, please contact the Data Protection Officer, Legal Services.

CCTV USER CHECKLIST

Property (Property where CCTV camera is located)	**Purpose of CCTV Camera** (i.e. primarily for security purposes/in order to ensure the safety and security of staff and visitors/ prevention and/or detection of crime.)	**Public Awareness** (In order to comply with Principle 1 of the Data Protection Act 1998 (fair and lawful obtaining and processing), individuals should be made aware that a CCTV system is in use. Please advise how this is done – signs displayed etc.)	**Nominated Officer** (The Supervising Officer for the CCTV System)	**Storage and Retention** (Where are images stored, who has access to the images and how long they are kept for?)	**Quality** (I.e. How often are the media changed/if quality not adequate for purpose who will this be reported to? /How long for repair or reinstatement if broken or damaged/Where will maintenance log be kept and who is responsible to check log?) Give Details
Premises office	Security purposes/in order to ensure the safety and security of staff and visitors/ prevention and/or detection of crime	Signage displayed	Site Manager	Stored: CCTV Hard Drive Viewed by: Leadership Team / Middle Leaders / Premises Staff Kept for: 28 days	The media will be changed every 28 Days
Network Manager's office	Security purposes/in order to ensure the safety and security of staff and visitors/ prevention and/or detection of crime	Signage displayed	Site Manager	Stored: CCTV Hard Drive Viewed by: Leadership Team / Middle Leaders / Premises Staff Kept for: 28 days	The media will be changed every 28 Days

Headteacher's Office	Security purposes/in order to ensure the safety and security of staff and visitors/ prevention and/or detection of crime	Signage displayed	Site Manager	Stored: CCTV Hard Drive Viewed by: Leadership Team / Middle Leaders / Premises Staff Kept for: 7 days	The media will be changed every 7 Days

Cardinal Heenan Catholic High School

CCTV POLICY

1. Purpose

1.1 The CCTV system installed at Cardinal Heenan Catholic High School will be used primarily for security purposes, in order to ensure the safety and security of staff and visitors. The system will also be used for prevention/detention of crime.

1.2 The CCTV system will monitor activity on Cardinal Heenan Catholic High School and the shared sixth form building.

2. Public Awareness

2.1 In order to comply with Principle 1 of the Data Protection Act 2018 (fair and lawful obtaining and processing), individuals will be made aware that a CCTV system is in use. A number of camera warning signs will be sited around the area. The signs will be clearly visible and legible.

3. Nominated Officers

3.1 The supervisory officer for Cardinal Heenan Catholic High School CCTV system will be the Site Manager. The system will be used and monitored by designated staff under the supervision of the Site Manager.

4. Storage and Retention

4.1 Images will be *stored on CCTV Hard Drive* and will only be viewed by the designated staff.

4.2 In accordance with Principle 5 of the Data Protection Act 1998, images will be kept only as long as necessary for the specified purpose. They will, therefore, be retained for 28 days. When this period expires the images will be removed or erased.

5. Quality

5.1 The media will be changed every 28 Days. If the quality of images is not adequate for the intended purpose, this will be reported to the Site Manager.

5.2 If a breakdown occurs, the camera will be repaired and reinstated as soon as possible.

5.3 A maintenance log for the system will be kept by the FM provider, Spie, and will be checked by the Site Manager.

Do's

- Follow this guidance or the approved code of practice.

- Inform the Information Commissioners Office (ICO) of the system. Please refer to page 7, Principle 2 as most council properties are covered corporately and therefore the ICO has been notified.

- Have a designated responsible person to manage the CCTV scheme (Site Manager).

- Ensure that the system is suitably managed and supervised in respect of GDPR, data protection issues, privacy, quality and storage of images for example.

- Display relevant warning signs in places where the system operates giving contact details.

- Review the system as a team to ensure that it is being used in accordance with this guidance or the approved code of practice.

- Ensure that staff are trained and understand the systems correct usage.

Don't

- Film areas that could amount to an infringement of personal privacy;

- Ignore subject access requests (an individual's written request to access information about themselves under the General Data Protection Regulation). A person identifiable on CCTV images may be entitled to view the footage and may make a request to do so;

- Use CCTV footage for any other purpose other than what it was originally used for, e.g. Prevention and detection of a crime, health and safety of pupils, staff and visitors;

- Use covert (i.e. where it is calculated to ensure that the persons are unaware) monitoring without seeking legal advice;

- Use Intrusive Surveillance at all (i.e. do not go inside someone's home, or car, or use surveillance equipment outside such places, which gives the same image or sound as if that person was inside their home or car;

- Use inadequate equipment. Blurred or indistinct images could constitute as inadequate data, whilst poorly maintained equipment may not provide legally sound evidence;

- Disclose data to third parties, unless it is lawful to do so;

- Systematically monitor people by use of CCTV but if this is the only method of obtaining the information that you need to obtain, seek prior authorisation under RIPA.