Guidelines for Use of Closed Circuit Television (CCTV) by Educational Establishments in Flintshire

Reviewed by Governors
March 2023

Schools should have due regard to this guidance to ensure that the use of CCTV complies with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and the Freedom of Information Act 2000

GUIDELINES FOR THE USE OF CCTV SYSTEMS IN FLINTSHIRE SCHOOLS

This Code of Practice (herein after referred to as "the Code") is issued by Flintshire County Council.
It is intended to regulate the management, operation and use of CCTV systems by Flintshire schools and to provide guidance as to good practice for users of CCTV systems.

The Code is based upon the CCTV Code of Practice published by the Information Commissioner, which sets out the standards that must be met if the requirements of the Data Protection Act 1998 is to be met. These are listed below:

Data should be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;
- Processed in accordance with individuals' rights;
- Secure;
- Not transferred to countries without adequate protection.

1. INTRODUCTION

1.1 These guidelines set out the accepted use and management of CCTV equipment and images to ensure schools comply with the Data Protection Act 1998, Human Rights Act 1998 and other legislation.

1.2 Images of people captured on CCTV where they can be easily identified may be regarded as personal data under the Data Protection Act 1998. This means that Flintshire schools must meet the requirements of the Act when using CCTV.

1.3 Schools should have due regard to the Code to ensure that they can justify their use of CCTV under the Data Protection Act 1998 and subsequent guidance released by the Information Commissioner's Office and under the Human Rights Act 1998.

1.4 The Code applies where open use of CCTV is intended in public areas. It does not apply to targeted or covert surveillance activities. Any operation of this kind may only be carried out with reference to the Regulation of Investigatory Powers Act (RIPA) in consultation with the Council's RIPA officer and/or the Police. For further details see section 7.

1.5 The Code applies to all CCTV systems, whether digital (recommended) or analogue.

1.6 The Code of Practice will be reviewed every two years or as legal advice changes.

1.7 The CCTV system in its entirety is owned by the school.

2. PURPOSE OF CCTV

2.1 Schools may wish to use CCTV for a number of reasons such as:

- to provide a safe and secure environment for pupils, staff and visitors when they are on school premises;
- to protect the school building(s) and assets;
- to support North Wales Police in a bid to deter and detect crime;
- to assist in identifying, apprehending and prosecuting offenders;
- to assist in managing the school and in monitoring those using its land and buildings;
- to assist, where appropriate, in disciplinary investigations and proceedings.

2.2 Before installing and using CCTV on school premises, the following steps should be taken:

- asses and document the appropriateness of, and reasons for, using CCTV;
- establish and document the purpose of the proposed scheme;
- establish and document who is responsible for day-to-day compliance with the Code;

- because CCTV involves the processing of personal data, ensure the scheme is included on the Data Protection Register under the school's notification with the office of the Information Commissioner.

3. RESPONSIBILITIES FOR CCTV OPERATION

3.1 Overall responsibility for CCTV systems operated in schools lies with the head teacher. CCTV systems must be managed and administered in accordance with the Code and any additional guidance issued by the Local Authority where necessary.

3.2 The day-to-day management of the CCTV scheme will be the responsibility of person(s) nominated by the head teacher and the site manager during the day and any designated members of staff at evenings, weekends and during school holidays.

3.3 Precautions must be in place to control access to CCTV equipment and to prevent unauthorised access and misuse. All staff with access to the system must ensure that they adhere to any guidance and security precautions.

4. LEGAL BASIS FOR USE OF CCTV SYSTEMS

4.1 The use of CCTV and the images recorded should comply with the Data Protection principles and must be:

- fairly and lawfully obtained;
- adequate, relevant and not excessive;
- accurate;
- used only for purposes about which people have been informed;
- secure and protected from unauthorised access;
- not held longer than required for the purposes they were recorded;
- accessible to data subjects where a valid request has been made under the Data Protection Act and where the images are defined as personal data.

4.2 In order to use CCTV, a school must have a legitimate basis for recording the personal data. The legitimate purposes for which CCTV would be in use in a school are, in general, the following:

- prevention and detection of crime, e.g., theft, arson and criminal damage;
- to protect the school buildings and assets;
- to increase the perception of safety and reduce the fear of crime;
- to assist in the management of the school in terms of the behaviour of pupils when constant supervision is not possible;
- to ensure the safety of pupils and others present on school premises and enhance positive behaviour of pupils, staff and visitors.

4.3 Schools must document the purposes for which CCTV is to be used on the premises.

4.4 The use of CCTV must be fair and must not be excessive or prejudicial to any individual or any group of individuals. In order for the use of CCTV to be fair, schools must inform people that CCTV is in use on their premises by means of notices.

4.5 The Human Rights Act gives every individual a right to private life and correspondence. This means that CCTV should not be used inappropriately and in areas where people could expect privacy. The Human Rights Act also makes it imperative that people are informed when CCTV is in operation.

5. ENSURING THAT USE OF CCTV IS FAIR

5.1 Schools should include the use of CCTV on their annual Data Protection notification (registration) to the Information Commissioner's Office as one of the purposes for which they use personal data.

5.2 Schools must only use CCTV for the purposes they have stated. CCTV or images produced from it should not be used for any other purposes, particularly purposes which could not reasonably be envisaged by individuals.

5.3 Prior to installing a system, it would be good practice if schools could consult with parents and pupils about the use of CCTV on the school site and with any other nearby residents or business owners who may be affected by its use.

5.4 Schools will ensure that pupils, staff and other people who use their buildings are informed of the use and purpose of CCTV. This should be done by means of clear and obvious notices placed around the school premises. Notices should include the following information:

- the identity of the Data Controller (the school);
- the purposes for which CCTV is being used, e.g., for the prevention or detection of crime;
- details of who to contact about the scheme and name/phone number where applicable.

5.5 The precise wording of a notice may vary, but suggested wordings are:

Warning premises are protected by closed circuit television. The images recorded are used for the purposes of crime prevention and public safety
Operator: Contact:

For your safety and security and for the prevention of crime, closed circuit television operates in this area.
Operator: Contact:

5.6 Compliant notices are available from the Local Authority at a minimal cost.

5.7 CCTV cameras must only record images on school premises and should not include any surrounding private property.

6. SELECTION, OPERATION AND SECURITY OF CCTV SYSTEMS

Selecting a system

6.1 The CCTV system chosen must be of sufficient quality to ensure that recordings and images produced are useable by the school and the Police. When choosing or updating a system, the latest Police guidance (which can be found on the Home Office website) should be used. In general:

- Schools should refer to the generic CCTV specification document available on moodle and seek advice from the Authority's CCTV Manager prior to installing any new CCTV systems or equipment.

- Digital systems are recommended as they provide good quality recordings and the capacity to produce clips and stills and to copy records to removable media.

- Equipment must work effectively together. For example, a high quality digital CCTV system can only be used to its full capacity if the cameras are also of a similar quality.

Operating the system

6.2 Cameras and equipment must be properly maintained and serviced and maintenance logs should be kept up to date. In the event of camera or equipment damage or break down there should be clear responsibility for getting the repairs carried out within a specific time period.

6.3 External cameras should be protected from vandalism by using preventative measures such as fitting anti-climb collars to camera mountings wherever possible.

6.4 Where removable media such as DVD or tape is used, it should be of a high quality and tapes should be replaced on a regular basis. Schools should not continue to use tapes once it becomes evident that the quality of the images has begun to deteriorate. Schools using DVD's should use the non re-writable type.

6.5 Cameras should be sited so that they capture images relevant to the purpose(s) for which the scheme has been established. Care should be taken that the view from a camera does not become obscured.

6.6 Where the location of the cameras and the time and date are displayed and recorded, these should be regularly checked for accuracy.

Security

6.7 CCTV recording equipment should be held in a separate, locked room where possible (or in a locked cupboard where this is not possible) and access must be strictly confined to authorised staff. Where other staff or visitors need to have access to the system, this should be documented.

6.8 If out of hours emergency maintenance is required the staff member in charge of the CCTV system must be satisfied of the identity of contractors before allowing access to the equipment.

6.9 Remote access to cameras via 'off air' access or via broadband links should be used sparingly. When accessing cameras from home over the Internet, staff should ensure that unauthorised persons cannot view the footage.

Retention of recordings

6.10 Recordings should only be held for a limited length of time and must be destroyed when their use is no longer required. A maximum retention period of 31 days is recommended but this may be extended where the recordings are required for an ongoing investigation.

6.11 For digital recording systems, images held on the hard drive will be overwritten on a recycling basis once the drive is full, and in any event should not be held for more that 31 days.

6.12 When the retention period has been reached images stored on removable media such as DVD or tape should be destroyed or wiped securely once the purpose of the recording is no longer relevant.

6.13 Recording media no longer in use must be securely destroyed.

7. COVERT MONITORING

7.1 CCTV should not be used covertly (i.e. without making people aware of it) as such an activity is governed by the Regulation of Investigatory Powers Act (RIPA). The police are able to carry out covert surveillance provided they follow the requirements of RIPA.

8. ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

8.1 Access to, and disclosure of, images recorded on CCTV must be restricted and carefully controlled. This will ensure that the rights of individuals are retained, and also ensure that the images can be used as evidence if required.

8.2 Images can only be disclosed in accordance with the purposes for which they were originally collected, and in accordance with the School's Notification to the Office of the Information Commissioner.

Access to Images

- Access to recorded images should be restricted to staff authorised to view them, and should not be made more widely available.
- Monitors displaying images from areas in which individuals would have an expectancy of privacy should only be seen by staff authorised to use the CCTV equipment.
- Viewing of recorded images should take place in a restricted area to which other employees, pupils etc. will not have access while viewing is occurring. All viewings must be properly documented (see appendices A and B).
- Images retained for evidence should be securely stored.

8.3 If media on which images are recorded is removed for viewing purposes, this must be documented (see appendix B). The following information must be documented when recording media is removed for viewing:

- Date and time media removed.
- Name of person removing the media.
- Name(s) of person(s) viewing the images.
- The name of the department to which the person viewing the images belongs or the organisation if the person is from outside the school.
- The reason for viewing the images.
- The date and time the media was returned to the system or secure storage.

Disclosure of Images

8.4 Disclosures to third parties will only be made in accordance with the purpose(s) for which the system is used and will be limited to:

- Police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.*
- Prosecution agencies.
- Relevant legal representatives.
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings).
- In exceptional cases, to others to assist in identification of a victim, witness or perpetrator in relation to a criminal incident.
- Members of staff involved with School disciplinary processes.

8.5 CCTV recordings should only be held by the school unless there is a legitimate reason to disclose them. Disclosure includes the viewing of images by someone who is not the operator of the system as well as the transfer of recordings to another organisation.

8.6 Records may need to be disclosed for the following reasons:

- to the police, for the prevention and detection of crime;
- to a court for legal proceedings;

- to a solicitor for legal proceedings.

8.7 Where recordings have been disclosed or viewed by an authorised third party the school must keep a record of:

- when the images were disclosed;
- why they have been disclosed;
- any crime incident number to which they refer;
- who the images have been disclosed to.

8.8 Viewing of CCTV recordings by the Police must be recorded in writing. Requests by the Police are actioned under section 29 of the Data Protection Act. The Police should provide a completed section 29 form stating that the information is required for the prevention and detection of crime. If a form is not available, or in an emergency, the school must record in writing when and why the information has been released.

8.9 Should a recording be required as evidence, a copy may be released to the Police. Where this occurs the recording will remain the property of the school. The date of the release and the purpose for which it is to be used must be recorded (see appendix B).

8.10 The Police may require the school to retain recordings beyond the recommended 31 day retention period for possible use as evidence in the future. Such records must be stored and indexed so that they can be retrieved when required.

8.11 Applications received from other outside bodies (e.g., solicitors) to view or release DVD's or tapes will be referred to the head teacher. In these circumstances, DVD's or tapes may be released where satisfactory evidence is produced showing that they are required for legal proceedings, a subject access request (see section 9) or in response to a Court Order.

8.12 DVD's or tapes will only be released to the media for use in the investigation of a specific crime and with the written agreement of the Police.

8.13 All requests for disclosure should be documented. If disclosure is denied, the reason should also be recorded.

8.14 In addition to the information required in section 8.7 above, the following should be documented (if applicable):

- If the images are being removed from the CCTV system or secure storage to another area, the location to which they are being transferred.
- Any crime incident number, if applicable.
- The signature of the person to whom the images have been transferred.

**The head teacher, or his/her designated representative, is the only person who can authorise disclosure of information to the police or other law enforcement agencies.*

9. SUBJECT ACCESS REQUESTS

9.1 Section 7 of the Data Protection Act 1998, gives individuals who are the subject of personal data the right to request access to it. This may include CCTV images.

9.2 Where a request has been made to view an image or recording, an application must be made in writing to the head teacher. The applicant should be provided with a Subject Access Request application form (see appendix C). The individual may wish to access either a still image or part of a recording. All Subject Access Requests are subject to the payment of a fee of £10.

9.3 Where third parties are included in the footage, they should be removed where this is technically possible. Where removal is not possible, their consent should be sought. Where consent is refused or where it is not possible to gain consent, a balanced decision needs to be made, taking conflicting interests into account, as to whether it is reasonable in all circumstances to release the information to the individual.

9.4 There is no obligation to provide information where a request has been made after CCTV records have been routinely destroyed in accordance with the Code - see 6.11 (i.e., for recordings that no longer exist). However, where a request has been made for recordings still in existence, they must not be destroyed until the request is complete.

9.5 For further information on dealing with requests under the Data Protection Act, the school's Data Protection policies should be consulted, along with County Council guidance. Where queries arise the Lifelong Learning Directorate Data Protection contact officer should be contacted for advice.

9.6 Schools must respond promptly and at least within 40 days of receiving the fee and sufficient information to identify the images requested.

9.7 If the school cannot comply with the request, the reasons must be documented and the requester must be advised of these in writing where possible.

9.8 Under the Freedom of Information Act 2000, a copy of these guidelines will be provided to anyone making a written request for it.

10. STAFF TRAINING

10.1 The head teacher will ensure that all staff with responsibility for handling CCTV images or recordings receive appropriate training on the operation and administration of the CCTV system. In addition, the head teacher will liaise with the Lifelong Learning Directorate's Data Protection contact officer to ensure training is provided on the impact of the Data Protection Act 1998 with regard to the system.

11. BREACHES OF SCHOOL GUIDELINES

11.1 Any breach or alleged breach of school guidelines on the use of CCTV by school staff or other individuals should be investigated by the head teacher.

11.2 An investigation should be carried out into any breaches and procedures reviewed or put in place to ensure that the situation does not arise again.

12. COMPLAINTS

12.1 Any complaints about the operation of the CCTV system should be addressed to those having day-to day responsibility, as listed in section 3 above, where they will be dealt with according to the school's standard complaints procedures.

12.2 If a complainant or enquirer is not satisfied with the response received, they should write to the head teacher.

Summary of Key Points

This code of practice will be reviewed every two years.

The CCTV system is owned, operated and maintained by the school.

Liaison meetings may be held with the Police and other law enforcement agencies if required.

Recording/recorded materials will be used properly, indexed, stored securely and destroyed after appropriate use.

Recorded materials required as evidence will be properly referenced, witnessed and packaged before copies are released to the Police.

Recorded materials will not be made available to the media for commercial or entertainment purposes.

Recorded materials will not be retained longer than is necessary.

CCTV should not be used for the purposes of covert surveillance

Any breaches of this Code of Practice will be reported to the head teacher who will carry out an investigation and take appropriate action as contained in this Code.

IF IN DOUBT SEEK ADVICE

CCTV GUIDANCE OR SIGNAGE:

Sherryl Burrows,
CCTV Manager
Tel: 01352 704490
E-mail: sherryl.burrows@flintshire.gov.uk

LIFELONG LEARNING DIRECTORATE DATA PROTECTION CONTACT OFFICER:

David Bridge
Records Manager
Tel: 01352 702178
E-mail: david.bridge@flintshire.gov.uk

APPENDIX A

RECORD OF VIEWING OF IMAGES BY AUTHORISED SCHOOL STAFF

_____ SCHOOL

Date and Time Image Viewed:

Date: / / Time: _ _: _ _

Name of Persons Viewing the Image:

Name: _____ Designation: _____

Reason(s) for the viewing:

_____

_____

_____

_____

Outcome, if any, of the viewing:

_____

_____

_____

_____

APPENDIX B

RECORD OF VIEWING BY THIRD PARTY (E.G. Police)

_____ SCHOOL

Date and Time Access Allowed:

Date: / / Time: _ _: _ _

Identification of all third parties who were allowed access:

_____

_____

Names of school staff present:

_____

_____

Reason for allowing access:

_____

_____

Crime Incident Number (if applicable):

_____

_____

Location of the Images:

_____

_____

Signature of Person Authorised to Collect the Copy (where appropriate):
……..

Date and Time Copy Created for Evidential Purposes:

Date: / / Time: _ _: _ _

Date and Time Copy returned to school system for secure storage:

Date: / / Time: _ _: _ _

APPENDIX C

RIGHT OF SUBJECT ACCESS APPLICATION FORM

SECTION 7 DATA PROTECTION ACT 1998

_____SCHOOL

Full Name: _____

Address: _____
_____
_____

Post Code: _____

Home Tel. Number: _____ Mobile: _____

Date of Birth: ___/___/___

Proof of Identity:

To help establish your identity, your application must be accompanied by official documentation such as a copy of your passport, vehicle registration document, a copy of your driving licence or a recent utilities bill showing you as the account holder

Photographic Means of Identification of Subject:

A recent full face photograph of yourself must also be enclosed with your application.

Date and Time Image Recorded:

Date: / / Time: _ _: _ _

Location: _____

To carry out a search for the images, a fee of £10.00 will be charged.

Please complete the above form, provide proof of identification, a recent photograph and attach a £10.00 cheque made payable to _____ School.

The head teacher will consider the request and respond within 28 days.