

Best Practice in the use of Closed Circuit Television (CCTV)

Closed Circuit Television (CCTV) surveillance is an increasing feature in our schools to assist in managing site security and student behaviour. The Data Protection Act 2000 (DPA) covers the processing of images captured on cameras and how these are handled and used. This document aims to provide schools with general best practice guidance, and offers suggestions on the standards schools should consider in order to minimise risk.

General Principles:

The school should comply with the Data Protection Act 1998 and CCTV Code of Practice 2008 where it uses CCTV systems. The following guidance, information, and suggested templates provide a framework for schools to work within where CCTV is being used.

Schools will need to fully address the following points to ensure they are compliant with legislation and operating to an appropriate standard:

There is reasonable justification before CCTV is installed and used.

An assessment of impact on people's privacy has been undertaken. For example, the CCTV must not invade neighbours privacy when viewing perimeter fencing.

A designated person will have legal responsibility for the scheme (known as the Data Controller).

The Data Controller (identified in 3 above) must fully understand their role and responsibilities, the legislation which governs the use of CCTV in school (including the requirements relating to the location & controlling of equipment, access to and use of the data captured etc)

The intended use of the CCTV should be documented and the system must not be used for anything other than this. For example, if the scheme is merely for site security (viewing perimeters) then images of individuals must not be taken.

The scheme must be notified to the Information Commissioners Office (ICO). For further information how to register (notify) under the Data Protection Act go to: www.ico.gov.uk

Each system should have documented procedures in place for its administration (the policy), which should include:

- ☐ Ensuring notification to ICO and your relevant Safeguarding Team 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.

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

Permanent or movable cameras should 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 (e.g. toilets/changing rooms) and CCTV may only be used in very extreme cases and this must not be undertaken without correct notification to the ICO and senior manager of the site (Head teacher / Building Managers for example).

The CCTV will only be used at relevant times; times when site security is at risk for example.

The equipment used should be maintained to ensure it is not tampered with and to provide reliable quality images.

No sound recording technology should be used.

Material should be stored in line with your policy document and not for longer than is necessary. It should be appropriately and securely deleted as soon as possible. For example, as soon as it is obvious that no crime has occurred, then the data should not be kept.

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

Each school should give careful consideration to which employees should be authorised to operate the system.

Images must not be released to third parties. Police may legitimately request images by way of a formal written request to the relevant person such as the Head teacher.

Individuals who are recorded may request access to the images, the procedure for this must be detailed within your policy document.

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

The CCTV systems must not be used to systematically monitor people. If this is required to obtain the information that is needed then authorisation under Regulation of Investigatory Powers Act (RIPA) 2000 will be required.

Each school should have a CCTV policy document. This document should also be considered within the context of the school safeguarding policy document.

Installation of the equipment may require a permit to work and or asbestos survey to be undertaken, where wiring is installed in ceiling voids etc it must not breach fire breaks as this would compromise the fire integrity of the building.

Appendix 1 (RAN21) Suggested Policy Document Template

Closed Circuit Television CCTV Policy Document for School

1. Introduction

The purpose of this document is to regulate the management, operation and use of CCTV systems in our school.

- 1.1 (INSERT NAME OF SCHOOL) uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, to prevent the loss or damage to property and to assist in the investigation of accidents, incidents and near misses.
- 1.2 The system comprises of **(insert how many)** number of fixed* and dome* cameras (*DELETE AS APPLICABLE).
- 1.3 The system has/does not* have sound recording capability. (*DELETE AS APPLICABLE)
- 1.4 The CCTV system is owned and operated by the school. (OR STATE ALTERNATIVES if ownership or operation is for example shared) and the deployment of which is determined by the school's leadership team.
- 1.5 The CCTV is monitored centrally from (INSERT LOCATION) by (INSERT NAME/POSITION OF DATA CONTROLLING OFFICER OR 3rd PARTY IF REMOTELY MONITORED).
- 1.6 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the school community.
- 1.7 The school's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated images and any sound recordings, is covered by the Data Protection Act 1998. This policy outlines the school's use of CCTV and how it complies with the Act.
- 1.8 All authorised operators and employees approved to access images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities as part of the requirements of this policy document, the schools safeguarding policies and procedures, e-safety information and the Data Protection Act. All employees are aware of the restrictions in relation to storage of, access to, and disclosure of, recorded images and sound. Failure to adhere to these requirements could lead to disciplinary action.

2. Statement of Intent

- 2.1 The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. Further information is available at:

http://www.ico.gov.uk/~media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx

- 2.2 CCTV warning signs will be clearly and prominently placed at all external entrances to the school, including main staff/pupil and visitor entrances and school gates, if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see appendix 3). In areas where CCTV is used, the school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.
- 2.3 The planning and design of the system has endeavoured to minimise any invasion of privacy and ensure that the Scheme will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will fully meet this brief or detect every single incident taking place in the areas of coverage.

3. Siting the Cameras

- 3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act, cameras will be regularly checked to ensure they have not been moved or tampered with in any way.
- 3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.
- 3.3 CCTV will not be used in classrooms with the exception of (INSERT AREA e.g. the isolation unit OR DELETE IF NOT APPLICABLE).
- 3.4 Members of staff upon request will have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.
- 3.5 Every effort will be made to ensure suitably competent contractors with the relevant knowledge and experience will be employed to install and maintain the equipment.

4. Covert Monitoring

- 4.1 The school may in exceptional circumstances set up covert monitoring. For example:
- i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;

- ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.
- 4.2 In these circumstances authorisation must be obtained from a member of the senior management team, who will seek advice from the schools Legal Information Management Officer before allowing such an operation to take place.
- 4.3 Covert monitoring must cease following completion of an investigation.
- 4.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets or changing areas.

5. Storage and Retention of CCTV images

- 5.1 Recorded data will not be retained for longer than is necessary, and will be deleted/erased appropriately and in line with approved procedures. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.
- 5.2 All retained data will be stored securely and access limited to authorised operators/staff only.

6. Access to CCTV images

- 6.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.
- 6.2 A list of staff authorised to view Images from this CCTV system will be held by the school.

7. Subject Access Requests (SAR)

- 7.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.
- 7.2 All requests must be made in writing to the Head teacher. Individuals submitting requests for access will have to provide sufficient information to enable the footage relating to them to be identified & isolated. For example, date, time and location.
- 7.3 The school will respond to requests within 40 calendar days of receiving the written request and fee.
- 7.4 A fee of £10 will charged per request. (OPTIONAL AT SCHOOLS DISCRETION)

- 7.5 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

8. Access to and Disclosure of Images to Third Parties

- 8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).
- 8.2 Requests should be made in writing to the Head teacher/Governing Body*. (*DELETE AS APPLICABLE)
- 8.3 The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. Complaints

- 9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Head teacher/Governing Body* in the first instance. (*DELETE AS APPLICABLE)
- 9.2 Failure of authorised operators/staff to comply with the requirements of this policy will lead to disciplinary action under the schools code of conduct.

10. Further Information

Further information on CCTV and its use is available from the following sources:

- ☐ CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- ☐ www.ico.gov.uk
- ☐ Regulation of Investigatory Powers Act (RIPA) 2000
- ☐ Data Protection Act 1998
- ☐ Crown Prosecution Service – www.cps.gov.uk

Appendix 2 (RAN21) – Checklist of Operation

The school CCTV system and the images produced by it are controlled in line with our policy, our data controller will notify the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998). The school has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of users of the site. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

Check Criteria	Date Checked/or Action Completed	By (Signature)	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
The name of the individual responsible for the operation of the system is _____.			
The system is checked to verify it produces clear images which the law enforcement bodies (usually the police) can use to investigate crime, these can easily be taken from the system when required.			
Staff and members of the school community are consulted about the proposal to install and or continued use of CCTV equipment.			
Cameras have been sited so that they provide clear images and limit the opportunity to be tampered with.			
Cameras are located in the following areas			
Cameras have been positioned to avoid intentionally capturing the images of persons not visiting the premises.			
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).			
Images from this CCTV system are securely stored in _____ and access is limited to the following authorised persons:			
Recorded images are retained for _____ days unless they form part of an incident under investigation.			
Procedure are in place to respond to the police or individuals making requests for access to data held.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix 3 (RAN21) – CCTV Signage

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- ☐ That the area is covered by CCTV surveillance and pictures are recorded
- ☐ The purpose of using CCTV
- ☐ The name of the school
- ☐ The contact telephone number or address of the systems operators for enquiries (this will either be the school or if monitored externally the details of the provider)
- ☐ Your signage must include a pictorial image identical to the one shown below

