CCTV in Schools

Guidance Document

Publication Date by LA: November 2016

Last reviewed: 2025

Document Control

Document Title: CCTV in Schools

Summary

Publication Date	November 2016
Related Legislation / Applicable Section of Legislation	Surveillance Code of Practice June 2013. Information Commissioners Office CCTV Code of Practice Data Protection Act 1998, Human Rights Act 1998 and other legislation.
Related Policies, Strategies, Guideline Documents	Information Governance, Data Protection Internal Audits
Replaces	CCTV Guidance for Schools November 2009
Joint Guidance Document (Yes/No)	Yes
Name of Partner(s) if joint	Schools
Guidance Document Owner/Author	Maria Tickle, IG Planning & Risk Manager

Review of Guidance Document

Last Review Date	
Review undertaken by	
Next Review Date	November 2018 (or when required)

Document Approvals

This document requires the following approvals.

Name	Title	Date of Issue	Version Number
Sandra Bowness	Assistant Director, Early Help & Schools	Nov 2016	1.0

1. Introduction

This is a guidance document and should be read in conjunction with the published Codes of Practice at point 10.

Schools use closed circuit television (CCTV) images to provide a safe and secure environment for pupils, staff and visitors, and for the prevention and detection of crime. This guidance relates to the use and management of CCTV. [NB: within this document, any reference made to school could also mean Academy. Any reference to Headteacher could also mean Principal.

It is recognised that operation of CCTV may be considered to infringe on the privacy of individuals. It is the schools responsibility to ensure that CCTV system complies with all relevant legislation, to ensure its legality and legitimacy.

There are a number of risks present when operating CCTV which need to be considered:

- **Data Protection Act 1998 (DPA):**

Employers should act in accordance with the DPA and its eight key principles. The Information Commissioners Office (ICO) enforces the DPA and breach of it may lead to sanctions and bad publicity for schools. Schools should also be conscious of the increased risk of receiving subject access requests (SARs) where monitoring is used. ICO Guidance for the Public

- **Human Rights Act 1998 (HRA):**

Schools should be particularly aware of the right to privacy which their employees, pupils and visitors have under the HRA as it applies directly to them. Schools must ensure that CCTV monitoring is not disproportionate or intrusive, as tribunals and courts will take this into account when making decisions.

Before installing CCTV for these purposes, your school should:

- carefully assess all alternative solutions.
- carry out a privacy impact assessment to assess how this will affect the right to privacy of pupils and staff. For further information on privacy impact assessments, visit the ICO website
- inform parents and pupils that CCTV is installed – failure to do so is likely to breach the Human Rights Act and the Data Protection Act.

This document summarises the accepted use and management of the CCTV equipment and images to ensure the school complies with the Data Protection Act 1998, Human Rights Act 1998, Information Commissioner's CCTV Code of Practice, and other legislation.

For the purposes of the Data Protection Act the 'Data Controller' is the School and the nominated person is the Headteacher. The Headteacher may, however, delegate responsibility for management of the System but remains accountable. Where this occurs, delegation must be clearly recorded and only to someone who has received appropriate training e.g. CCTV/SIA Licence or other approved training.

The operation of CCTV should be included on the schools registration with the Information Commissioners Office.

2. Guidance

Schools should be aware of and comply with published guidance and standards for CCTV operation (see Point 10: Supporting Documents). The guidance covers both recording and viewing images including viewing live images.

The purpose of having CCTV monitoring can be for a number of reasons e.g. for the prevention and detection of crime.

The school should make every effort to position cameras to ensure they only cover school premises.

Schools should ensure that they are aware of the location of cameras and any impact this has on the privacy of individuals or neighbouring properties. If, for any reason, neighbouring domestic areas that border the schools property are included in the camera view, the occupants of the property should be consulted prior to any recording or recording for those areas will need to be disabled.

The School should clearly display signs in the vicinity of the cameras so that pupils, staff and visitors are aware they are entering an area covered by CCTV.

Signage in the building should state that:

- The name of the school responsible for the CCTV scheme and contact details
- The purpose of having CCTV in place e.g. the prevention and detection of crime

Use of the CCTV must not be excessive or unreasonable. When considering whether to use CCTV footage, the Headteacher must decide whether the use is legitimate in view of the Schools clearly stated objectives. Images can be used retroactively to monitor persons who pose a significant risk to themselves or others.

3. Covert Recording/Surveillance

The school should be aware of the legal requirements relating to covert surveillance and ensure this is a proportional response when used. Surveillance is covert if it is carried out in a manner that is calculated to ensure that the person subject to the surveillance is unaware that it is taking place.

In order to comply with Principle 1 of the DPA, any organisations that record images and sound must inform individuals prior to any recordings taking place. Failure to display signage for CCTV or other recording systems could infer that it is being undertaken covertly.

Use of covert recording should be for a specific purpose and have a documented authorisation process in place signed by the Headteacher, in advance.

4. Access to and Disclosure of Images

Only staff authorised and trained to view CCTV images should be in the room when footage is being displayed on a screen. Images should only be reviewed by the Headteacher or other qualified/trained staff e.g. CCTV/SIA license or other approved training. The school should maintain a list of these

individuals. Schools may wish to consider buying in this service or pooling resources to get an individual trained for a group of schools.

Images of staff should only be accessed if an event occurs that the School cannot be expected to ignore such as criminal activity, to assist in the detection of professional misconduct or behaviour that puts others at risk. The legality of use must be established to ensure it meets the necessary thresholds (see proportionate and reasonable use).

Monitors displaying images from areas in which individuals would have an expectancy of privacy should only be seen by staff authorised and trained to use the equipment. No other individual should have access to or undertake monitoring of the system.

Viewing of recorded images should take place in a restricted area to which other employees will not have access while viewing is occurring. If media on which images are recorded are removed for viewing purposes this should be documented.

Images retained for evidence should be securely stored.

The following information should be documented when media are viewed, once authorised by the Headteacher:

1. Date and time
2. The name(s) of the person(s) viewing the images.
3. The name of the organisation to which the person viewing the images belongs if the person does not work for the school.
4. The reason for viewing the images.

Disclosures to third parties should only be made in accordance with the purpose(s) for which the system is used and with a clear legal basis. This would include disclosures to the Police and those requested under subject access (SAR). There are specific rules relating to such disclosures.

5. Retention

There should be a clear retention policy in place for images and a process to retain images outside this retention authorised by the Headteacher.

6. Staff Training

If the Headteacher has delegated responsibility, that person is tasked with day-to-day responsibility of the systems. It is the Headteachers responsibility to ensure that staff are trained in the operation or administration of CCTV.

The delegated responsibility at Lowerplace is Hollingworth IT service.

7. Responsibility for CCTV System & Complaints

Overall responsibility for the CCTV system lies with the Headteacher.

Complaints and enquiries about the operation of the CCTV systems should be made using the School Complaints Procedure.

Enquiries relating to the Data Protection Act should be handled in line with school procedures.

8. Proportionate & Reasonable Use

Use of the CCTV system must not be excessive or unreasonable. When considering whether or not

to use CCTV footage, the Headteacher must decide whether the use is legitimate in view of the School's clearly stated objectives. If a particular request is made for access to footage, even if it is considered to be in line with the objectives, the Headteacher must decide whether it is proportionate. For example, it may be necessary to use the footage where there are no alternative ways to resolve the issue in hand. These considerations are needed to ensure that any CCTV footage used is admissible as evidence.

Where there are issues of a disciplinary nature, CCTV should not be used unless no other evidence exists and the system is used for verification purposes.

Necessary thresholds, and whether schools can use the footage in respect of school proceedings, can only be established at the point in time and its use must be justified, necessary and proportionate in each case. An assumption cannot be made that because the footage is in existence it can be used whenever a situation relating to professional misconduct occurs.

9. Discipline

Individuals with any responsibility under the terms of this Document and who have any involvement with the CCTV will be subject to their organisations discipline rules. Any breach of this guidance or any aspect of confidentiality will be dealt with in accordance with those rules. The Headteacher or delegated person will accept primary responsibility for ensuring there is no breach of security and that the School complies with the requirements for lawful use of CCTV. He/she has day to day responsibility for the management of the system and for enforcing the discipline rules. Non-compliance may lead, where appropriate, to the instigation of criminal proceedings.

10. Supporting Documents

Including but not limited to:

Information Commissioners Office Code of Practice	https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
The Home Office Surveillance Camera Code of Practice	https://www.gov.uk/government/organisations/surveillance-camera-commissioner
Surveillance Commissioner – self assessment tool	self-assessment tool.
Information Commissioners Office Code – Employment Practices Code	https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf