Apex Primary School

CCTV Code of Practice Policy

Reviewed: September 2025 Next review: September 2028

Contents

Code of Practice on CCTV use for School Staff

Introduction

1.1 This Code of Practice explains the School's use of Closed Circuit Television (CCTV) surveillance and recording. It does not form part of any employment contract and the Governing Body reserves the right to amend it at any time in line with the School's evolving requirements and concerns.

1.2 Following a Privacy Impact Assessment (PIA) (outlined in Appendix B) and consultation with governors, staff, parents and those who frequently and regularly use the School's premises, the governing body decided to operate CCTV in the School. The Privacy Impact Assessment will be periodically reviewed and updated annually.

1.3 The School intends that its use of CCTV will contribute to:

- the general security of the School providing a safe and secure environment for pupils, staff and other site users;
- protecting the School's property and assets, including by collecting and storing evidence for insurance purposes;
- helping the School to manage pupil disciplinary and staff conduct issues;
- informing the School's arrangements for fire and general safety;
- assisting with the detection, deterrence, and prevention of crime.

1.4 The CCTV system and any data it collects may be used to train those operating the system and to assist investigations into any missing person.

1.5 It is advisable that School personnel entrusted with responsibility for CCTV equipment and monitoring will receive appropriate training on Data Protection Act 1998 (DPA) compliance; the Freedom of Information Act 2000 (FOI); Human Rights Act 1998 (HRA) and the privacy implications of operating the CCTV system. They will be subject to a confidentiality requirement both during and post employment.

1.6 School's CCTV system is owned and operated by Apex Secondary School registered with the Information Commissioner and all data collected by it is covered by the DPA. This Code of Practice implements the Information Commissioner's Office (ICO) CCTV Code of Practice which is available from the Information Commissioner's website.

Legal Considerations

2.1 Staff, pupils and other School users may be reassured that the School takes privacy and data protection issues seriously and will only operate a CCTV system in the school if :

2.2 the operation is in line with this Code of Practice, the DPA, the HRA and the School's other legal obligations; there is reasonable and proper cause to believe that CCTV operation is a necessary and proportionate means of addressing serious concerns about safety, security and/or wellbeing;

2.3 CCTV will be used to the extent that it is necessary to address such serious concerns and the operation of the CCTV will occur in a professional, responsible, sensitive and unobtrusive manner.

Statement of practice

3.1 Location of Cameras

CCTV cameras are installed in locations where the School believes surveillance is a necessary and proportionate means to assist with managing certain significant issues and concerns. Where possible, CCTV cameras are sited to cause minimal intrusion into individuals' privacy while fulfilling the aims of surveillance.

Locations of CCTV cameras are listed at Appendix A to this Code of Practice. Notices advising that CCTV is operating will be prominently displayed at these locations before cameras commence operating.

3.2 Sound Recording

The CCTV system does currently have sound recording enabled. Before sound recording is enabled anywhere on School premises, notices will be prominently displayed in all relevant locations, advising that sound recording is in operation. Use of sound recording will be considered only in highly exceptional circumstances.

3.3 Covert Monitoring

School will undertake covert recording only in exceptional circumstances and after obtaining written authorisation from the Headteacher. Before giving this authorisation the Headteacher will satisfy themselves that:

- There is good cause to suspect that an illegal activity or serious misconduct is taking place or is about to take place and/or that an individual is/will be at serious risk of harm

- There is reasonable and proper cause to believe that covert CCTV recording is a necessary and proportionate means of investigating and addressing those concerns; and

- Notifying School users that CCTV recording is taking place would seriously compromise the School's ability to investigate its concerns and to take appropriate action.

- Where covert monitoring is used it will only be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring and only for specific activities. All occasions of covert monitoring will be fully documented, recording who made the decision to use covert monitoring, the dates and time this occurred and reasons why this was necessary.

3.1 Date and Time recording

Checking and recording procedures will be implemented to ensure date and time settings on the CCTV system are accurate.

Limits on the use of CCTV

4.1 CCTV will NOT be used to:

- monitor the progress of staff or pupils in the ordinary course of school activities;
- observe staff working practices, performance or time-keeping; or
- assist in the day-to-day management of staff.
- capture images of pupils changing

4.2 Individuals operating equipment have been instructed not to direct cameras to capture images within private homes, private gardens and other areas of private property. Unless an immediate response to events is required and has given specific authorisation, cameras will not be used to follow individuals, their property or a specific group of individuals. The Headtacher is expected to take legal advice before authorising use in these circumstances.

4.3 The School will not arrange for CCTV cameras to be sited in any washing or toilet facilities, private offices or changing rooms ("private spaces") unless this is necessary for the investigation of a serious crime or in circumstances of serious risk to health and safety or serious risk to the operations of the School. In the exceptional circumstances of these serious risks, CCTV recording in private spaces may be a proportionate means of preventing or mitigating such risks.

4.4 School will ensure that where cameras are used in private spaces, public notices are prominently displayed to publicise CCTV surveillance is in operation in those private spaces. The School will not display a public notice in those exceptional situations where it undertakes covert recording and in those instances surveillance will occur only where it is authorised under this Code of Practice and accords with the relevant law.

Further Processing of CCTV Data

5.1 Only authorised School personnel may view images obtained from the School's CCTV system. Viewings must occur in secure restricted areas; on each viewing details of the date, time, reason for viewing together with the name of the person viewing the images and details of any outcomes must be recorded by Jeremy Barlow, Assistant Headteacher.

5.2 Subject Access Requests

CCTV equipment at the School records images of people who use School premises and those persons have the right to view the recording of themselves and receive a copy of their images. Requesters are required to visit the School with photograph identification (normally drivers licence or passport) and provide details of the relevant date and time the image was taken, so that the School can be certain it is obtaining the correct information and releasing it to the correct person.

5.3 School will ensure that where staff and other persons who use School premises make unambiguous requests for access to images of themselves and do so in accordance with this Code, the School will provide copies within 40 calendar days of the request. The School reserves the right to charge for any such request, the maximum charge that will be levied is £10 per request.

5.4 When complying with any subject access request, the School may edit images and/or footage to protect identities of other persons if the School is unable to obtain consent to the disclosure from those other persons. The School may refuse requests where it is impossible to adequately protect the identities of others, or where complying with the request would put a criminal investigation at risk.

5.5 **Freedom of Information Requests**

Where a request for CCTV footage is a request under the Freedom of Information Act 2000 the School will respond to such a request within 20 working days giving details of any exemption that the School believes is applicable to the request.

5.6 **Third Party Requests**

Disclosure of CCTV images to third parties will be limited to the following: -

- Law enforcement agencies;
- Prosecution agencies;
- Legal representatives;
- HR professionals who are under a continuing professional and contractual duty of confidentiality to the School and who have given appropriate guarantees regarding the security measures they will take in relation to the images;
- The media in order to assist the Police; and
- The individuals who are the subject of the CCTV images.

5.7 Except in the most exceptional circumstances, CCTV images will not be passed to any third party for editing, or made more widely available (e.g. to the media, posted on the internet etc.). If the School intends images to be made more widely available, the Headteacher will make that decision and the reason for the decision will be documented.

Use of CCTV images as Evidence

6.1 Where in the reasonable belief of the School management, CCTV evidence tends to suggest that an employee's actions are likely to constitute gross misconduct, the CCTV evidence may be used against an employee in disciplinary proceedings. The employee will be given a chance to see the footage and comment on it.

6.2 In the course of covert CCTV monitoring, the CCTV system may capture footage of misconduct or malpractice which is unrelated to the objectives of the covert monitoring operation. Such evidence may only be used against an individual where the misconduct or malpractice uncovered amounts to a criminal offence or poses a significant danger to any individual; or in the case of a School employee, may amount to gross misconduct.

6.3 **Objections to Processing**

Individuals have a right to object to data processing of their own personal data that causes, or is likely to cause, unwarranted and substantial damage or distress and in the most serious cases may require the School to stop (or not to begin) the processing in question. Such objections must be put in writing, specifying with evidence why the data processing has, will or is deemed likely to have this effect.

6.4 Objections which relate to processing data collected by the School's CCTV system will be referred to the Headteacher who will

determine how the School will respond to the objection. Within 21 days of receiving an objection, the Headteacher will provide a response that sets out the [decision and where the objection is not accepted the letter
will provide reasons for the decision. The reasons may include factors that show the objection was unjustified or factors that show processing the data was necessary to avoid some significant injustice or harm. Usually the Headteacher should consider suspending processing data or restricted processing of data while the objection is being considered.

6.5 If within 21 days the individual requires, in writing, that the decision be reconsidered, the Headteacher shall reconsider giving regard to any new relevant matters. Where the objection is from a person who at the time is involved in an internal complaint or grievance against the Principal/Headteacher, matters relating to objection to processing should be considered by a nominated school governor. All staff involved in operating the CCTV system will be trained to recognise an objection to processing.

Retention of CCTV footage

7.1 Images of CCTV footage will be stored securely and access will be restricted to authorised personnel. Images will not be retained for longer than necessary, usually two weeks but this may be longer where the images are required for evidential purposes in legal proceedings. Where it becomes necessary to take hard copies of recordings, these will be indexed, stored securely and destroyed after appropriate use.

Complaints

8.1 Any complaints or enquiries about the operation of CCTV within the School should, in the first instance, be addressed to the Headteacher.

Breaches of the CCTV Code of Practice by School staff will be investigated by the Headteacher and may result in appropriate disciplinary action.

Appendix A

Locations of CCTV cameras

Main front
Main entrance
Side gates
Upper left staircase
Main reception
Playground angle 1,2,3,4 & 5
Upper right staircase
Office
Hall

Appendix B

The Employment Practices Code (a code of practice published by the ICO) sets out detailed guidance on the use of CCTV in the workplace, including:

- Carrying out a Privacy impact assessment. This could be invaluable in justifying the case for CCTV usage. Ensure a record is kept of the assessment. It should identify :

    1. the purpose behind monitoring and the likely benefits
    2. the likely adverse impacts
    3. alternative ways in which the purpose might be achieved
    4. the obligations which will arise from monitoring individuals (e.g. notification, managing data in line with DPA, subject access requests)
    5. whether the decision would be ultimately justifiable

- Ensure those involved in monitoring are aware of their obligations. These individuals should also be subject to strict confidentiality and security obligations.

- Make School users aware of the nature and extent of the monitoring and have a written policy in place, which should:

    1. be readily available to School users; and
    2. be signed for to signify agreement and understanding

- Be clear about privacy levels (e.g. no cameras in private areas etc.)

- Give individuals the chance to be heard. Allow them to voice concerns in confidence and explain and challenge any CCTV evidence that is to be used as part of a disciplinary process.

- Store and process information in line with the DPA. Data must be relevant, not excessive, securely stored and not kept for longer than is necessary.

- Deal with Subject Access Requests ("SARS") promptly. Those whose images are captured have a right to a copy of the CCTV footage. SAR's must be responded to by the employer within 40 days of receipt of the request.