Icknield High School

CCTV Policy

July 2026

Contents Page

1 Aims and Objectives……..3

2 General principles……3

3 Location of cameras……4

4 Management and Retention……4

5 Storage and Retention of images……5

6 Disclosure of images……5

7 Misuse of CCTV system……6

8 Review, monitoring and complaints……6

1. Aims and Objectives

1.1 The purpose of this policy is to regulate the management, operation, and use of Closed Circuit Television (CCTV) and associated technology at Icknield High School.

1.2 The CCTV system is installed to:

- Protect school buildings and assets, both during and after school hours.
- Promote the health, safety, and welfare of staff, students, and visitors.
- Reduce the incidence of crime and anti-social behaviour (including theft and vandalism).
- Assist law enforcement agencies to deter, detect, and investigate crime.
- Support the school's behaviour policy.
- Support the identification, apprehension, and prosecution of offenders.
- Enhance the management of the school, including automated number plate recognition (ANPR) for gate entry.

1.3 The system will be operated in line with safeguarding principles, ensuring privacy and dignity for all individuals on school premises. This includes the use of audio recording and limited facial recognition technology for safeguarding and security purposes, ensuring compliance with privacy laws.

2. General Principles

2.1 This policy complies with the:

- UK General Data Protection Regulation (GDPR).
- Data Protection Act 2018.
- CCTV Code of Practice.

2.2 The use of CCTV will be conducted professionally, ethically, and in compliance with legal standards. Diversion of CCTV for purposes outside the stated aims is prohibited. Audio recording will adhere to GDPR and the Data Protection Act 2018 and will only be used for legitimate safeguarding and security purposes. The system will also comply with ICO Guidance on Surveillance and Biometric Data (2023) and respect Article 8 of the Human Rights Act 1998. No personal data beyond video and audio footage is stored.

2.3 CCTV access will only be granted to authorised staff, as outlined in this policy. Requests from law enforcement or others for access will be carefully reviewed to ensure legal compliance.

2.4 A **Data Protection Impact Assessment (DPIA)** will be conducted before the installation of new cameras or significant changes to the system. DPIAs are mandatory for any processing involving audio or biometric data.

3. Location of Cameras

3.1 CCTV cameras will be installed to achieve the stated objectives, in prominent, clearly visible locations, with signage to inform staff, students, and visitors that CCTV and audio recording is in operation.

3.2 Cameras will not monitor areas outside school grounds unless unavoidable. Efforts will be made to respect privacy and avoid capturing public areas or adjacent private property.

3.3 IT rooms, entry points, and other high-risk areas will have CCTV coverage for the protection of equipment and premises security.

3.4 Automated Number Plate Recognition (ANPR) will be used exclusively for gate entry purposes. Vehicle registration details will not be stored in the access database, and related footage will follow the same retention policy as other recordings.

3.5 Audio Recording: Audio recording is enabled on selected cameras to enhance safeguarding and security. Clear signage will indicate areas where audio is active. Audio data will follow the same retention period as video (28 days unless required for investigation). Access is restricted to authorised staff.

3.6 Facial Recognition: Facial recognition technology is used on a limited number of cameras to log corridor presence for safeguarding purposes. No biometric templates or personal identifiers are stored beyond footage. Logs are anonymised and retained under the same retention policy.

4. Management and Retention

4.1 The CCTV system will be managed by a member of the Senior Leadership Team (SLT). Authorised personnel include:

- Site Team.
- Network Management Team.
- Pastoral Team.
- Leadership Team members.

4.2 Authorised staff will receive training on system operation, data protection, and safeguarding responsibilities. Training records will be maintained and updated annually.

4.3 A designated safeguarding lead (DSL) will oversee the integration of safeguarding considerations into CCTV operations. All authorised staff will receive training on handling CCTV, audio and biometric data responsibly.

5. Storage and Retention of Images

5.1 CCTV recordings will be retained for no longer than 28 days unless required for a specific investigation. Images related to ongoing criminal or safeguarding investigations may be retained for the duration of the investigation or as legally required. This retention policy applies equally to audio recordings and facial recognition logs.

5.2 Data security measures include:

- Restricted access to CCTV systems.
- Use of password-protected systems in secure, monitored areas.
- Permissions for copying or downloading footage limited to authorised staff.
- Secure deletion of data when no longer required.

6. Disclosure of Images

6.1 Requests for CCTV images will be managed in accordance with the GDPR and the Data Protection Act 2018: Requests may include audio and biometric data, which will be handled under the same principles of privacy and proportionality.

- Subject Access Requests (SARs) will be reviewed under the Subject Access Request Policy. Requests will be limited to footage containing the requester only, unless it is possible to anonymise or obtain consent from other individuals captured in the footage.
- If anonymisation or consent is impractical, the request will be assessed for reasonableness, ensuring the privacy rights of all individuals are respected.

6.2 Before sharing any footage, consideration will be given to whether doing so could lead to further incidents, risks to individuals, or safeguarding concerns. Where such risks are identified and deemed significant, the footage may not be shared. This decision will be documented, including the rationale and any legal advice obtained.

6.3 Any disclosure must balance the individual's rights with safeguarding and privacy considerations. A record will be kept of all disclosures, including:

- The requester's details.
- The justification for disclosure.
- Actions taken, including access granted or refused.

7. Misuse of CCTV System

7.1 Misuse of the CCTV system is strictly prohibited and may constitute a criminal offence.

7.2 Staff who breach this policy will be subject to disciplinary action in line with the school's disciplinary procedures.

8. Review, Monitoring, and Complaints

8.1 This policy and the CCTV system will be reviewed annually to ensure compliance with legal and ethical standards.

8.2 Complaints related to CCTV operation will be handled through the School's Complaints Policy.

8.3 The school will regularly assess the effectiveness of CCTV in meeting its stated objectives and consult stakeholders, including staff, students, and parents, as part of the review process.

Appendix A: Data Protection Impact Assessment (DPIA) Template

This template must be completed before implementing any new CCTV features, including audio recording or facial recognition, to ensure compliance with UK GDPR and Data Protection Act 2018.

1. Purpose of Processing

Describe why the CCTV system, audio recording, or facial recognition is being introduced and its intended benefits.

2. Description of Processing

Detail what data will be collected (e.g., video, audio, biometric logs), how it will be stored, and who will have access.

3. Necessity and Proportionality

Explain why this processing is necessary and proportionate to achieve the stated objectives.

4. Risk Assessment

Identify potential risks to individuals' privacy and data protection rights.

5. Mitigation Measures

Outline steps to reduce risks, such as signage, restricted access, retention limits, and staff training.

6. Sign-Off

Name, role, and date of the person approving the DPIA.