Highlands
School & Sixth Form

Dare to flourish

CCTV policy

APPROVED

Governor Committee	Finance and Resources
Reviewed on	May 2026
Next review	May 2028

Contents

Section 1: Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- make members of the school community feel safe.
- protect members of the school community from harm to themselves or to their property.
- deter criminality in the school.
- protect school assets and buildings.
- assist police to deter and detect crime.
- determine the cause of accidents.
- assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings.
- assist in the defence of any litigation proceedings.
- support the operational effectiveness of the school and provide evidence for improvement, for example patterns of movement and behaviour.

The CCTV system will not be used to:

- encroach on an individual's right to privacy.
- monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms).
- follow particular individuals, unless there is an ongoing emergency incident occurring.
- pursue any other purposes than the ones stated above.

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

1.2 Lawful Basis for Processing

The school processes CCTV data (personal data and special category data) under the following lawful bases defined by the UK GDPR:

- **Article 6(1)(e) – Public Task:** The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school (e.g., maintaining a safe environment for education).
- **Article 6(1)(f) – Legitimate Interests:** The processing is necessary for the legitimate interests of the school or a third party (e.g., the protection of school property), except where such interests are overridden by the fundamental rights and freedoms of the data subject.
- **Article 9(2)(g) – Substantial Public Interest:** Where the school processes "Special Category Data" (e.g., footage revealing ethnic origin or health), it does so on the basis of substantial public interest, specifically for the purposes of safeguarding children and preventing/detecting unlawful acts.

Section 2. Relevant legislation and guidance

This policy is based on:

2.1 Legislation

This policy is informed by the following key legislation:

- The UK Data Protection Framework: Consisting of the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025
- The Protection of Freedoms Act 2012 (and the Surveillance Camera Code of Practice 2021)
- The Human Rights Act 1998 (specifically Article 8: Right to Privacy)
- The Equality Act 2010
- The Freedom of Information Act 2000

2.2 Guidance

The school will also take into account the following statutory and non-statutory guidance:

- **ICO: Guide to the UK General Data Protection Regulation (UK GDPR)** – for general data handling principles.
- **ICO: Video Surveillance (including CCTV) Guidance** – the primary guidance for using cameras in public spaces.
- **Biometrics and Surveillance Camera Commissioner: The 12 Guiding Principles** – ensuring the system is transparent and proportionate.
- **DfE: Search, Screening and Confiscation (2022)** – if CCTV is used to identify prohibited items on school grounds.
- **DfE: Keeping Children Safe in Education (KCSIE)** – ensuring CCTV usage aligns with safeguarding obligations.
- Surveillance Camera Code of Practice (2021)

Section 3. Definitions

Surveillance: the act of watching a person or a place.

CCTV: closed circuit television; video cameras used for surveillance.

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance.

Section 4. Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

Additionally, the proper authorisation forms from the Home Office will be completed and retained where necessary.

Section 5. Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Cameras are located in:

- corridors, stairwells and communal areas such as the dining hall, main hall and student common room.

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

- Identifies the school as the operator of the CCTV system.
- Identifies the school as the data controller.
- Provides contact details for the school.
- Indicates the stated purpose as "for the purposes of public safety and crime prevention"

Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

Section 6. Roles and responsibilities

6.1 The governing board

The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The headteacher

The headteacher will:

- take responsibility for all day-to-day leadership and management of the CCTV system.
- liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified.
- ensure that the guidance set out in this policy is followed by all staff.
- review the CCTV policy to check that the school is compliant with legislation.
- ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection.
- sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of a data protection impact assessment.
- decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties.

6.3 The data protection officer

The data protection officer (DPO) will:

- train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection.
- train all staff to recognise a subject access request.
- deal with subject access requests in line with the Data Protection Act 2018 / UK GDPR.
- monitor compliance with UK data protection law.
- advise on and assist the school with carrying out data protection impact assessments.
- act as a point of contact for communications from the Information Commissioner's Office.
- conduct data protection impact assessments.
- ensure data is handled in accordance with data protection legislation.
- ensure footage is obtained in a legal, fair and transparent manner.
- ensure footage is destroyed when it falls out of the retention period.
- ensure CCTV usage is integrated into the school's wider safeguarding approach, ensuring footage of vulnerable children is handled with extra sensitivity.
- keep accurate records of all data processing activities and make the records public on request.
- inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information.
- ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified.
- ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces.
- carry out annual checks to determine whether footage is being stored accurately, and being deleted after the retention period.
- receive and consider requests for third-party access to CCTV footage.

6.4 The system manager

The system manager will:

- take care of the day-to-day maintenance and operation of the CCTV system.
- oversee the security of the CCTV system and footage.
- check the system for faults and security flaws half termly.
- ensure the data and time stamps are accurate half termly.

Section 7. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is registered with the Information Commissioner's Office.

The system does not record audio.

Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

Section 8. Storage of CCTV footage

Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 30 days for litigation or safeguarding reasons. For example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recordings will be downloaded to a secure folder and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required. It will be marked with a new deletion date (usually 6 years for legal claims or until the student is 25 for safeguarding cases).

The DPO will carry out annual checks to determine whether footage is being stored accurately, and being deleted after the retention period.

Section 9. Access to CCTV footage

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

9.1 Staff access

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence, and will face disciplinary action.

9.2 Subject access requests (SAR)

According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves. The school will conduct "reasonable and proportionate" searches

Upon receiving the request the school will conduct reasonable and proportionate searches for images, issue a receipt within five working days and will then respond without undue delay and at the latest within one calendar month. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members or in more complex cases.

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO in writing. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

9.3 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the headteacher and the DPO.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the DPO.

Section 10. Data protection impact assessment (DPIA)

The school recognizes that the use of a surveillance camera system is a high-risk activity that impacts the privacy of students, staff, and visitors. In accordance with UK GDPR, a Data Protection Impact Assessment (DPIA) will be conducted in line with the ICO's standard template:

- **Prior to the installation** of any new CCTV or surveillance equipment.
- **Before making significant changes** to the existing system, such as moving cameras, changing software, or upgrading to higher-resolution hardware.
- **If new high-risk features are introduced**, such as the trial of facial recognition or automated tracking.
- **Annually**, as part of the review of the system's necessity and proportionality.

The DPIA will involve the DPO and the System Manager to identify and minimize privacy risks. If a DPIA identifies a high risk that cannot be mitigated, the school will consult the Information Commissioner's Office

Section 11. Security

- The system manager will be responsible for overseeing the security of the CCTV system and footage
- The system will be checked for faults half-termly
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

Section 12. Complaints

Complaints should be directed to the headteacher or the DPO and should be made according to the school's complaints policy.

Section 13. Monitoring

The policy will be reviewed every two years by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

Section 14. Links to other policies

- Data protection policy
- Behaviour policy
- Safeguarding policy