CCTV Policy

Applicable to:	✓	Astley Community High School
	✓	Seaton Sluice Middle School
	✓	Whytrig Middle School
Approval body:	Resources Committee	

Status:

Statutory policy or document	No
Review frequency	Governing Body to determine
Approval by	Governing Body to determine

Publication:

Statutory requirement to publish on school website	No
Agreed to publish on school website	Yes

Review:

Frequency	**Next Review Due**
Every three years	Autumn 2026

Version Control:

Author	Creation Date	Version	Status
Data and Curriculum Services Manager (AD)	22 August 2018	0.1	Initial draft compliant with GDPR, based on WMS policy (December 2014)
Changed by	**Revision Date**		
Business Manager (BW)	21 September 2018	1.0	Final approved version for publication
Business Manager (BW)	1 October 2019	1.1	Authorisation to view images restricted to senior leaders only, on advice from DPO
Business Manager (BW)	21 October 2019	2.0	Final approved version for publication
Business Manager (BW)	3 August 2020	2.1	Annual review, change to review frequency only
Business Manager (BW)	15 September 2020	3.0	Final approved version for publication
Business Director (BW)	30 November 2022	3.1	Updated to include audio recording
Business Director (BW)	20 October 2023	3.2	Fully rewritten in line with The Key for Leaders model policy (March 2023)
Business Director (BW)	6 November 2023	4.0	Final approved version for publication

1 Aims

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

2 Statement of intent

2.1 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 our schools
- 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

2.2 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

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

2.4 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.

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

2.6 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.

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

3 Relevant legislation and guidance

3.1 This policy is based on:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010
- Surveillance Camera Code of Practice (2021)

4 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

5 Covert surveillance

5.1 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.

6 Location of the cameras

6.1 The system comprises fixed position cameras, monitors, digital recorders, and public information signs. Cameras will be located at strategic points on the school sites in order to achieve the aims of the CCTV system as set out above, principally at the entrance and exit point of sites and buildings, and also at some internal positions.

6.2 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 federation as the operator of the CCTV system
- identifies the federation as the data controller
- provides contact details for the federation

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

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

7 Roles and responsibilities

7.1 The **governing body**:

- has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

7.2 The **Executive Headteacher** will:

- take responsibility for all day-to-day leadership and management of the CCTV system
- liaise with the federation's Business Manager - Data and Curriculum Support and 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 the federation's Business Manager - Data and Curriculum Support and/or 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 the federation's Business Manager - Data and Curriculum Support and DPO, whether to comply with disclosure of footage requests from third parties

7.3 The **Business Manager - Data and Curriculum Support** (with support from the 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 Freedom of Information Act (2000)
- monitor compliance with UK data protection law
- act as a point of contact for communications from the Information Commissioner's Office (ICO)
- 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
- 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 federation, what their rights are, and how the federation 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 termly 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

7.4 The **Business Manager - ICT and Infrastructure**, in their role as 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 on a termly basis
- ensure the data and time stamps are accurate on a termly basis

8 Operation of the CCTV system

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

8.2 The system is registered with the ICO.

8.3 The system records audio.

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

9 Storage of CCTV footage

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

9.2 On occasion footage may be retained for longer than 30 days, 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.

9.3 Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

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

9.5 Once a hard drive has reached the end of its use it will be erased prior to disposal. All hard drives and recorders shall remain the property of the federation until disposal and destruction.

10 Access to images and audio recordings

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

10.2 Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.

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

<u>Staff Access</u>

10.4 Authorisation to view images and/or listen to audio recordings will be restricted to members of the Senior Leadership Team (SLT), Student Progress Leaders and Heads of Year. These people may authorise the viewing of images and/or listening to audio recordings by other members of staff only when it is necessary to fulfil the objectives of the system, for example to identify a person in an image or from the sound of their voice.

10.5 Only the Executive Headteacher or members of the SLT may authorise the viewing of images and/or listening to audio recordings by non-staff members, and only where it is necessary for the purposes of meeting the objectives of the system.

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

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

Subject Access Requests (SAR)

10.8 According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

10.9 Upon receiving the request the federation will immediately issue a receipt and will then respond within 30 days during term time. The federation reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

10.10 All staff have received training to recognise SARs. When a SAR is received staff should inform the Business Manager - Data and Curriculum Support 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 federation staff in locating the footage.

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

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

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

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

10.15 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.

10.16 Individuals wishing to make a 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.

Third Party Access

10.17 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies, where images and /or audio recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media, where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images or voices have been recorded and retained, unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings
- Emergency services, in connection with the investigation of an accident

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

10.19 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).

10.20 All requests for access should be set out in writing and sent to the Executive Headteacher.

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

10.22 The Business Manager - Data and Curriculum Support will ensure that any disclosures that are made are done in compliance with UK GDPR.

10.23 All disclosures will be recorded by the Business Manager - Data and Curriculum Support.

11 Data protection impact assessment (DPIA)

11.1 The federation follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

11.2 The system is used only for the purpose of fulfilling its aims as set out above.

11.3 When the CCTV system is replaced, developed or upgraded, a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

11.4 The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the Business Manager - Data and Curriculum Support.

11.5 Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

11.6 A DPIA will be undertaken annually and/or whenever existing cameras are moved or new cameras are installed.

11.7 If any security risks are identified in the course of the DPIA, the federation will address them as soon as possible.

12 Security

12.1 The Business Manager - ICT and Infrastructure will be responsible for overseeing the security of the CCTV system and footage.

12.2 The system will be checked for faults once a term.

12.3 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.

12.4 Footage will be stored securely and encrypted wherever possible.

12.5 CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use.

12.6 Proper cyber security measures will be put in place to protect the footage from cyber attacks.

12.7 Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible.

13 Complaints

13.1 Complaints regarding the federation's CCTV systems should be made in line with the federation's Complaints Procedure.