ELAN Surveillance and CCTV Schemes Document

Document Control

Document Information

	Information
Document Name	*ELAN Surveillance and CCTV Schemes Document*
Document Author	*Clive farmer*
Document Approval	*Operations, Estates & HR (for GDPR)*
Document Status	*Version 1*
Publication Date	*14.07.2025*
Review Date	*14.07.2026*
Distribution	*ELAN Schools operating or considering CCTV systems, Staff portal*

Version Control

Version	***Issue Date***	***Amended by***	***Comments***
1	*July 2025*	*Headteacher*	*New Policy*

1.0 Introduction

1.1 Extend Learning Academies Network (ELAN) is committed to safeguarding and promoting the safe use of Close Circuit Television Cameras (CCTV) for the welfare of our pupils, staff, and visitors. Each school within the Trust has a separate approach to CCTV that will form part of its own procedures, which can be found on the school's individual website. This statement outlines the approach schools should take when installing, using, and reviewing CCTV where it has been assessed by the school to be a requirement.

1.2 We use Surveillance and CCTV systems to:

- protect School buildings and their assets.
- increase personal safety and reduce the fear of crime.
- support the police in deterring and detecting crime.
- assist in managing the school.

1.3 The systems will not be used:

- to provide recorded images for the world-wide-web.
- to record sound.
- for any automated decision taking

1.4 The following policies are also relevant to this document:

Signpost	Document Title	Responsibility
Policy	ELAN Data Protection Policy (including GDPR)	ELAN HR
	ELAN Complaints Policy	ELAN HR

1.5 The appendices to this document contain further information and tools to assist schools in its implementation. These are:

- Appendix 1: CCTV Signage
- Appendix 2: Individual School CCTV Schedule
- Appendix 3: Surveillance System Access Log
- Appendix 4: Surveillance Camera Code of Practice
- Appendix 5: Surveillance and CCTV Policy [TEMPLATE FOR SCHOOLS]

NOTE: A school Surveillance and CCTV Policy is to be put in place across all ELAN schools if operating or considering the installation of surveillance or CCTV equipment in accordance with this document.

2. Definitions

2.1 **"the School"** means member Schools of the Extend Learning Academies Network (ELAN) that operate CCTV and surveillance systems.

2.2 **"Data Controller"** means the School's Data Controller (Headteacher).

2.3 **"Data Protection Officer"** the Trust is designated as a public authority or body for the purposes of Data Protection. This means that the Trust must have a Data Protection Officer (DPO).

2.4 **"Surveillance systems"** means monitoring the movements and behaviour of individuals; this can include video, audio, or live footage e.g., real-time recordings and live streams. For the purpose of this document only video and audio footage will be applicable.

2.5 **"Surveillance staff"** means school staff, which may include senior leadership or administrators or premises staff, with the skills and permission to manage and operate surveillance systems.

3.0 Statement of Intent

3.1 Surveillance systems are registered with the Information Commissioner's Office (ICO) under the terms of the Data Protection Act 2018. The ELAN will comply with the requirements both of the Data Protection Act and the ICO's CCTV Code of Practice. The Trust will treat all surveillance schemes and all information, documents and recordings obtained and used as data which are protected by the Act.

The Trust will register with the ICO and pay the appropriate fee on behalf of the schools. You can search the register here https://ico.org.uk/ESDWebPages/Search

3.2 The Trust will ensure privacy statements are updated and relevant.

3.3 Warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by School CCTV, by ELAN school schools operating CCTV.

3.4 Materials or knowledge secured as a result of CCTV or access control systems will not be used for any commercial purpose. Data will only be released for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

3.5 Systems are planned and designed to give maximum effectiveness, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. CCTV systems may include fixed or mobile cameras located around School sites.

3.6 Cameras will not focus on private homes, gardens, and other areas of private property. Cameras will be positioned to avoid capturing the images of persons not visiting the premises.

3.7 Unless an immediate response to events is required, cameras will not be directed at individuals, their property, or a specific group of individuals, without authorisation being obtained through an application for the use of directed surveillance, as set out in the Regulation of Investigatory Power Act 2000. Authorising Officers for the ELAN are the Chief Executive Officer (Adam Matthews) and the Data Protection Officer (Heidi

Neal-Millar). Approval must be obtained from a Justice of the Peace in accordance with Home Office guidance.

3.8 CCTV systems which make use of wireless communication links (e.g., transmitting images between cameras and a receiver) should ensure that these signals are encrypted to prevent interception.

3.9 CCTV systems which can transmit images over the internet (e.g., to allow viewing from a remote location) should ensure that these signals are encrypted to prevent interception and also require some form of authentication for access (e.g., a username and secure password).

3.10 Schools must ensure that cameras and systems produce clear images which law enforcement bodies (usually the police) can use to investigate crime, and these can easily be taken from the system when required.

3.11 The ELAN requires each of its school's operating CCTV systems to have a CCTV Policy in place.

3.12 If installing or extending CCTV a privacy impact assessment should be undertaken looking at the pressing need of the system, and if it will address the issues, and whether its proposed use has a lawful basis and is justified, necessary and proportionate.

A privacy impact assessment will be undertaken by each school's leadership team and local governing body (LGB) in liaising with the Trust GDPR Lead and Data Protection Officer to ensure compliance.

4. Roles and responsibilities

4.1 Data Protection Officer (DPO)

As a Trust we are data controllers in law and are required to appoint a Data Protection Officer. Our DPO is Heidi Neal-Millar (Head of HR).

The role of the Data Protection Officer (DPO) includes:

- Register CCTV with the Information Commissioner's Office.
- Dealing with freedom of information requests and subject access requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive, and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the UK GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity, and making these records public upon request.

- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Reporting to Trustees.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's data protection impact assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the Board of Trustees.

4.2 **Data Controller (The Headteacher)**

The school is the data controller. The Headteacher therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

4.3 The head teacher may nominate a member of school staff with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

4.4 The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate, and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration, and disclosure – especially when processing over networks.

4.5 The role of the Headteacher includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Undertakes, and has in place a Data Protection Impact Assessment before CCTV is installed or operated on the school premises.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

4.6 **The School operating Surveillance and CCTV Schemes**

The school will develop a school policy to meet its statutory and non-statutory obligations and management use of surveillance and CCTV system on its premises in accordance with the ELAN Surveillance and CCTV Document. This policy will be published on the school website.

5.0 Purpose and justification

5.1 The school will only use surveillance cameras for the safety and security of the school and its staff, pupils, and visitors.

5.2 Surveillance will be used as a deterrent for violent behaviour and damage to the school.

5.3 The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.

5.4 If the surveillance and CCTV systems fulfil their purpose and are no longer required, the school will deactivate them.

6.0 Data Protection

6.1 Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a Data Protection Impact Assessment (DPIA), or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interests assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
    - Further processing for archiving data in the public interest
    - Scientific or historical research
    - Statistical purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

6.2 The use of surveillance cameras, CCTV, and biometric systems, will be critically analysed using a DPIA, in consultation with the DPO.

6.3 A DPIA will be carried out prior to the installation of any surveillance, CCTV, or biometric system. A DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.

A template DPIA is available from the IOC website https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

6.4 Identify any additional measures to mitigate those risks.

6.5 Sensitive data obtained via biometric technology will be processed via special conditions (listed in Article 9 of the UK GDPR).

6.6 If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

6.7 Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

6.8 The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

6.9 If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek amendments.

6.10 Surveillance and CCTV systems will not be intrusive. Pupils, staff, and visitors will be made aware of the following:

- Whenever they are being monitored by a surveillance camera system
- Who is undertaking the activity
- The purpose for which the associated information is being used

6.11 The use of any video conferencing technology will be fair and transparent. Any pupils and staff who are part of any video conference calls will be informed of its purpose, and recording and publication of any video to an indefinite audience will be consented to and will not be used outside of the intended purpose.

7.0 Management of Surveillance systems

7.1 Surveillance systems will be administered and managed by the Data Controller, in accordance with the principles and objectives expressed in the code. The Data Controller is responsible for undertaking systematic checks of the management, operation, and retention of data and recording such checks on the Surveillance Log in accordance with this document.

7.2 Surveillance systems will be operated 24 hours each day, every day of the year.

7.3 Surveillance system controls and hardware will only be accessed by Surveillance staff or authorised personnel. Full details of access must be recorded in the School's Surveillance log (see Appendices for template log).

7.4 Day-to-day management is the responsibility of designated Surveillance staff. Surveillance staff will:

- check and confirm the efficiency of the system regularly including checking that cameras are functional and not obscured, recording and overwrite functions are as designed
- ensuring appropriate technical, physical, and organisational security of systems
- system maintenance is up to date

7.5 Cameras will be pointed and focused on fixed points agreed in advance by the Headteacher of each school. Only managers with responsibility for recorded images on authority from the Headteacher of each school shall be allowed to modify camera positions in response to a particular event or circumstances that is deemed to require surveillance. The CCTV system will not be used for covert surveillance unless specifically directed by authorised law enforcement agencies.

7.5 **CCTV footage will only be retained for a maximum of 30 days**. This means the right of erasure may not apply as erasure will happen automatically after 30 days. On occasion, we may need to retain data for a longer period, for example, where a law enforcement body is investigating a crime and asks for it to be preserved, to give them opportunity to view the information as part of an active investigation or where the school is investigating an incident. After this time, we will permanently delete the data through secure methods.

8.0 Covert and audio recording

8.1 The covert surveillance activities of public authorities are not covered here because they are governed by Regulation of Investigatory Powers legislation. This type of recording is covert and directed at an individual or individuals (Example: The police using covert surveillance equipment to monitor and record the activities of a suspected drug dealer to identify if related offences are committed.

8.2 The use of audio recording, particularly where it is continuous, will, in most situations, be considered more privacy intrusive than purely visual recording. Its use will therefore require much greater justification.

8.3 Audio recording will only be used where:

8.3.1 The school has identified a need or issue which can be characterised as a pressing social need and can evidence that this need must be addressed.

8.3.2 The school has considered other less privacy intrusive methods of addressing the need.

8.3.3 Having reviewed the other less privacy intrusive methods, the school has concluded that these will not appropriately address the identified issue and the only way to address the issue is through the use of audio recording.

8.3.4 The school should ensure that at the point of purchase of the audio system all appropriate privacy by design methods have been incorporated into the system. If you have already bought the system, you should look to see if you can incorporate any privacy by design technologies.

8.3.5 If the school is using audio recording, they should ensure the system they have bought provides a high enough quality of recording to achieve the stated aim.

8.3.6 The school should make it clear to data subjects that audio recording is taking place, over and above any visual recording which is already occurring.

9.0 Subject Access Requests (SARs)

9.1 Individuals have the right to request access to video footage relating to themselves under the Data Protection Act 2018.

9.2 Where possible, requests for Data Subject Access should be made in writing to the ELAN Data Protection Officer.

9.3 Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example, date, time, and location.

9.4 The Trust will immediately indicate receipt and then respond within one calendar month of receiving the request.

9.5 If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The appropriate representative must take appropriate measures to ensure that the footage is restricted in this way.

9.5 The Trust reserves the right to refuse access to video footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

9.6 If the footage contains images of other individuals, then the school or Trust must consider whether:

9.6.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals.

9.6.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

9.6.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

9.7 If all options have been considered and the School/Trust still consider there to be a risk to others from the requester viewing the video, the Trust may decline the request to view the video (although relevant exemptions in the Data Protection Act 2018 will need to be identified by the School/Trust provided to the requester).

9.8 A record must be kept, and held securely, of all disclosures which sets out:

- When the request was made.
- The process followed by the nominated representative in determining whether the images contained third parties.
- The considerations as to whether to allow access to those images.
- The individuals that were permitted to view the images and when; and
- Whether a copy of the images was provided, and if so to whom, when and in what format

9.9 The School or the Trust should not provide copies of the video to others unless instructed to do so in law or there is no risk to individuals who may be identifiable from the video.

10.0 Access to and disclosure to other third parties

10.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the Trust where these would reasonably need access to the data (e.g., investigators) and with the correct authorisation.

10.2 Requests from third parties should be made in writing to the Headteacher or the Data Protection Officer. However, regard must also be given to the following statement:

- *Consideration should always be given to the safeguarding and best interest of pupils. Data Protection should not be used as an excuse to prevent the viewing of images if there is an overwhelming need. All disclosures and the reasons for release should be recorded*.

10.3 The data may be used within the Trust's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures. This will be communicated to staff through the Trust's Privacy Notices.

11.0 Breaches

11.1 Any breach of this policy will be investigated by the Headteacher and/or the Trust's Data Protection Officer in line with the Trust's Personal Data Breach Policy.

12.0 Review of Policy and CCTV System

12.1 Schools operating CCTV and Surveillance equipment will ensure that they have in place a relevant policy in line with the ELAN CCTV and Surveillance Document.

12.2 Schools will ensure that the privacy impact statement relating to their setting remains relevant, by annual review.

13.0 Misuse of CCTV systems

13.1 The misuse of CCTV systems could constitute a criminal offence. Any member of staff who breaches the contents of this documents may be subject to disciplinary action.

14.0 Complaints

14.1 Any complaints about the School's surveillance systems can be made via the Trust's Complaints Policy.

Appendix 1: CCTV Signage

(Print on yellow paper) or ensure similar signage is displayed)



CCTV

Images are being monitored for the purpose of public safety, crime prevention, detection, and the prosecution of offenders.

This scheme is controlled by

Extend Learning Academies Network

For further information please see the Trust's Data Protection Policy on its website

extendlearning.org

Appendix 2: Individual School CCTV Schedule

SCHOOL NAME	CCTV (Yes/No)	Number of cameras		Named individual responsible for system	Named roles with authority to view images on CCTV* (e.g., Head teacher, Administrator, Caretaker)	Record Function (e.g., continuous, motion)	Storage location (e.g., School Office)	Image retention period (e.g., 30 days max)	Service and Maintenance Contractor (School contract)
		External	Internal						
Banwell Primary School	Yes	5	0	Claire Pocock	Headteacher	Motion Sensor / Continuous Motion	School Office / HT Office / PPA Office	Unsure	KIS
Bournville Primary School	Yes	10	17	Marie Berry	SLT, Administrators, Caretaker	Continuous	School Office	20 days	Coomber Security
Locking Primary School	No								
Mead Vale Primary School	Yes	7	2	Jo Jaloszynski	SLT	Continuous	SLT Office	25 days	None in place
Mendip Green Primary School	No								
Milton Park Primary School	Yes	7	0	Katharine Jordan	SLT, Pastoral Team	Continuous	Headteacher's office	30 days	Multi-Security
Oldmixon Primary School	Yes	8	1	Corinna Sutton	SLT, Office Administrator, Caretaker	Continuous /Motion	School Office	Not known	Computer Cubed
Walliscote Primary School	No								
Windwhistle Primary School	Yes	18	0	Wayne Hollowood	Headteacher, Deputy Head, Asst. Head, Caretaker, Office Administrator	Motion Sensor / Continuous Motion	SMSA Office	21 days	Multi-Security Services – Only until April.

**or authorised to view for identification*

Appendix 3: Surveillance Systems Access Log

Name of person accessing system	Purpose of access	Date	Time	Identity checked by	Visit approved by	Notes: To include details of any data removed

Appendix 4: Surveillance Camera Code of Practice

The 12 guiding principles from the Surveillance Camera Code of Practice:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, and used
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Surveillance and CCTV Policy
For Windwhistle Primary School

Written by:	ELAN Estates Manager	
Reviewed by:	Local Governing Body of Windwhistle Primary School	Date: 14.07.2025
Ratified by:	Name: John Porter Signed by: 	Date: 14.07.2025
Review:	Annually	
Next Review Due by:	July 2025	

Document Control
Document Information

	Information
Document Name	*Surveillance and CCTV Policy*
Document Author	*Estates*
Document Approval	*Operations Manager*
Document Status	*Version 1.0*
Publication Date	*June 2025*
Review Date	*June 2026*
Distribution	*Website /General*

Version Control

Version	Issue Date	Amended by	Comments
1	June 2025	Headteacher	New Policy

Contents

1. Statement of intent 18

2. Legal framework 18

3. Definitions 19

4. Roles and responsibilities 19

5. Purpose and justification 21

6. Data protection 22

7. Protocols 23

8. Security 24

10. Signage and Privacy Notices 25

10. Code of practice 25

11. Access 26

12. Monitoring and review 28

1. Statement of intent

At Windwhistle Primary School, we take our responsibility towards the safety of staff, visitors, and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with the UK GDPR.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff, and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

2. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- 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
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004

- Equality Act 2010

This policy operates in conjunction with the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'

The following policies, procedures and documents are also relevant to this Policy:

Signpost	Document Title	Responsibility
Policy	ELAN Data Protection Policy (including GDPR)	ELAN HR
	ELAN Complaints Policy	ELAN HR

[DRAFTING NOTE: Add any school policy documents to the table that might be relevant, e.g., School Security Policy; Online Safety Policy etc.]

3. Definitions

For the purpose of this policy the following definitions are given for the below terms:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio, or live footage e.g., real-time recordings and live streams. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – Surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000.
- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

The school does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

- **Biometric data** – data which is related to the physiological characteristics of a person, which confirm the unique identification of that person, such as fingerprint recognition, facial recognition (FRT), or iris recognition.

4. Roles and responsibilities

The role of the Data Protection Officer (DPO for the Trust is Heidi Neal-Millar)

- Dealing with freedom of information requests and subject access requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive, and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the UK GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity, and making these records public upon request.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the school, e.g., the governing board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's data protection impact assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the governing board.

The school is the data controller. The Headteacher therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate, and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration, and disclosure – especially when processing over networks.

The role of the headteacher includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

5. Purpose and justification

The school will only use surveillance cameras for the safety and security of the school and its staff, pupils, and visitors.

Surveillance will be used as a deterrent for violent behaviour and damage to the school.

The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.

If the surveillance and CCTV systems fulfil their purpose and are no longer required, the school will deactivate them.

The school has identified a need for CCTV externally. We have outlined below the reason(s) we use CCTV around our site:

(a) To reduce the fear of crime: Individuals work on their own in the building for significant parts of the day, and frequently the building is locked up at night by individuals. The presence of CCTV will provide a degree of assurance to individuals that the personal risk is reduced.

(b) To deter and prevent crime: There have been a small number of instances of anti-social behaviour, for example, individuals being abusive and, or refusing to leave the premises when requested to do so, or attempting to enter the premises when events are taking place or when the school is closed. It is intended that CCTV will act as a deterrent.

(c) To protect property: The presence of CCTV is intended to reduce crime. There have been a number of incidents which may well have been prevented by the presence of CCTV, including vandalism to the school buildings/infrastructure and parked vehicles, theft of School and personal property from the building and vehicles, and graffiti on exterior walls.

(d) Provide assistance in the detection of crime: in the event that any criminal incidents of any kind do occur, to provide high quality evidence which may assist in identifying

individuals involved and where appropriate detecting crime and apprehension and prosecution of offenders.

(e) To improve and provide assistance with issues relating to the health and safety of pupils, staff, and visitors: it is intended that in the event of any incident which may raise Health and Safety concerns, which CCTV may assist in determining the cause of the incident and any measures which need to be taken as a result of incidents.

(f) To assist in child protection by deterring inappropriate behaviour and providing assurances to staff, volunteers, and parents that evidence from CCTV may be available should the need arise to investigate an alleged or actual Child Protection incident.

6. Data protection

Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a DPIA, or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interests assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:

- Further processing for archiving data in the public interest
- Scientific or historical research
- Statistical purposes

- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The use of surveillance cameras, CCTV, and biometric systems will be critically analysed using a DPIA, in consultation with the DPO.

A DPIA will be carried out prior to the installation of any surveillance, CCTV, or biometric system. A DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

Sensitive data obtained via biometric technology will be processed via special conditions (listed in Article 9 of the UK GDPR).

If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek amendments.

Surveillance and CCTV systems will not be intrusive. Pupils, staff and visitors will be made aware of the following:

- Whenever they are being monitored by a surveillance camera system
- Who is undertaking the activity
- The purpose for which the associated information is being used

The use of any video conferencing technology will be fair and transparent. Any pupils and staff who are part of any video conference calls will be informed of its purpose, and recording and publication of any video to an indefinite audience will be consented to and will not be used outside of the intended purpose.

FRT will be justifiable, proportionate, and able to address specific needs.

7. Protocols

The surveillance system will be registered with the ICO in line with data protection legislation.

The surveillance system is a closed digital system.

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. Warning signs will be more prominent in

areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

8. Security

Access to the surveillance system, software and data will be strictly limited to authorised operators, and will be password protected, and where appropriate, will be encrypted.

In exceptional cases where large amounts of information need to be collected and retained, the school will consider using cloud storage. This will be secure and only accessible to authorised individuals.

The school's authorised CCTV system operators are:

- **Heidi Hudd, Headteacher**
- **Wayne Hollowood, data processor, site operative**

The main control facility is kept secure and locked when not in use.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

Surveillance and CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times.

The DPO and Headteacher will decide when to record footage, e.g., a continuous loop outside the school grounds to deter intruders.

Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

The ability to produce copies of information will be limited to the appropriate staff.

Any unnecessary footage captured will be securely deleted from the school system.

Each system will have a separate audio and visual system that can be run independently of one another. The school will not record audio unless it has:

- Identified a particular need or issue and can evidence that this need must be addressed by audio recording.
- Considered other less privacy intrusive methods of achieving this need.
- Reviewed the other less privacy intrusive methods and concluded that these will not appropriately address the identified issue and the only way to do so is via the use of audio recording.

Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

Visual access through desk top computers are located in the main office, Headteacher's office, Deputy Headteacher's office and the site operative's office.

10. Signage and Privacy Notices

It is a requirement of the Data Protection Act 2018, to notify people entering a CCTV protected area to inform that that the area is monitored by CCTV and that pictures are recorded. The CCTV sign should include the following:

That the area is covered by CCTV surveillance and pictures are recorded

The purpose of using CCTV

The name of the School

The contact telephone number and/or address for enquiries

Warning signs are placed at all access routes to areas covered by the school's CCTV

The school's use of CCTV is covered by a privacy notice which can be found on the School Website.

10. Code of practice

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school notifies all pupils, staff, and visitors of the purpose for collecting surveillance data via notice boards, signs, letters, and emails.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All surveillance footage will be kept for 30 days maximum for security purposes; the headteacher and the data controller are responsible for keeping the records secure and allowing access.

The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils, and visitors.

The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils, and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available on the school's website.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point which enables people to request information and submit complaints via the DPO.
- Have clear responsibility and accountability procedures for images and information collected, held, and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up to date.

11. Access

Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

All disks and hard drives containing images belong to, and remain the property of, the school.

Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

Individuals have the right to have personal data erased if:

- The data is no longer necessary for the original purpose it was collected for.

- They are relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.
- The data has been processed unlawfully.
- There is a specific legal obligation.

There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- Where the processing is needed for the performance of a task in the public interest or an official authority.
- Certain research activities.
- Compliance with a specific legal obligation.

As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by the school or they object to way it was processed.

Data can be restricted by either:

- Moving the data to another processing system.
- Making the data unavailable to users.
- Temporarily removing published data from a website.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a ‘reasonable fee’ to comply with requests for further copies of the same information. The individual will either be provided with a permanent copy of the information or allowed to view the information.

Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

Where a request is manifestly unfounded, excessive, or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by no more than an additional 20 working days. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

Where data requests contain the personal data of a separate individual, the rights and freedoms of others will be protected by asking for their consent or removing specific footage where appropriate.

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Requests for access or disclosure will be recorded and the headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

12. Monitoring and review

This policy will be monitored and reviewed on an annual basis by the DPO and the headteacher.

The headteacher will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.

The headteacher will communicate changes to this policy to all members of staff.