CCTV Policy & Data Protection Impact Assessment

Unity
Trust
Courage
Curiosity
Respect
Kindness

A community for learning. Raising expectations. Fulfilling high standards.

Revised: **30th March 2025**

The policy is to be reviewed by: **January 2027**

Headteacher: **Mrs Gemma Hillier**

Data Protection Officer: **Nicola Cook**

Contents

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 grounds
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents, injury or serious behaviour breaches
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defence of any litigation proceedings

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 will be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant legislation & guidance

This policy is based on:

2.1 Legislation

- 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

2.2 Guidance

- Surveillance Camera Code of Practice (2021)

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

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.

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:

- Facing the playground
- Facing the school playing field
- Facing the car park
- Facing the footpath from the front entrance
- Facing the front door
- Inside the School entrance lobby
- Inside the Inclusion Corridor
- Inside Sapphire intervention room
- Inside Emerald intervention room
- Inside the Music room

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage is highly visible on all entry points into the school grounds and located next to light switches in inside intervention/music rooms.

Cameras are not and will not be aimed off school grounds into public spaces without the explicit permission of the landowner. The cameras will not be aimed into people's private property. If this is unavoidable, the areas of private property will be notified and the

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

6. Roles & 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
- 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
- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- 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 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 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

6.3 The data protection officer

The data protection officer (DPO) will:

- 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
- 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

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 termly
- Ensure the data and time stamps are accurate termly

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 will not record audio.

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

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 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 stored within the CCTV system database and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required. The CCTV playback is only available via one PC within the school and only able to be opened by Admin staff.

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

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 that footage is not able to distinguish individuals outside of the office.

9.1 Staff Access

The following members of staff have authorisation to access the CCTV footage:

- The headteacher: Gemma Hillier
- The deputy head: Vicki Marshall
- The data protection officer: Nicola Cook
- The system manager (Office staff): Claire Weaver & Charlie Lenton
- Anyone with express permission of the headteacher

CCTV footage will only be accessed from one PC in the school office work device, or from the visual display monitor.

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.

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

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.

10. Data protection impact assessment

The school 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.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

If 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.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the Headteacher, Mrs Gemma Hillier.

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.

A new DPIA will be done whenever cameras are moved, or new cameras are installed.

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

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 once a term
- 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

12. Complaints

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

complaints policy.

13. Monitoring

The policy will be reviewed every 2 years by the Headteacher to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

14. Links to other policies

- Data protection policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding policy

15. Data Protection Impact Assessment

Why we need a DPIA

Widmer End Community Combined School operates a CCTV system. As such, we must consider the privacy implications of such a system. The completion of the Data Protection Impact Assessment highlights some of the key implications.

A Data Protection Impact Assessment is also recommended by the Surveillance Camera Code of Practice which sets out the guiding principles that should be applied when CCTV systems are in place to ensure that privacy risks are minimised whilst ensuring the aims of the CCTV system are met.

This Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for the CCTV system and the impact it may have on individual privacy.

This Data Protection Impact Assessment helps determine whether the system can be justified as proportionate to the needs of the school. In undertaking this Data Protection Impact Assessment, Widmer End Community Combined School has considered its obligations under Data Protection Law.

We recognise that changes do occur and on this basis, good practice recommends that the school review its Data

Protection Impact Assessment alongside the CCTV policy. The school recognises that it is good practice to undertake a Data Protection Impact Assessment before a system is put in place and follows the surveillance commissioner's passport to compliance.

CCTV consistently delivers benefits in terms of improved health and safety and security. It complements other security measures which are in place within the school.

CCTV aims to achieve the following:

- 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 grounds
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents, injury or serious behaviour breaches
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defence of any litigation proceedings

Parents have the assurance that their children are safe whilst in school. Parents are aware that with CCTV there is the potential for behavior at school to improve.

Nature of the Data Processing

The CCTV system provides the school with video pictures from 12 fixed based cameras located throughout the school site and the images will be captured on a Digital Video Recorder (DVR) system. The CCTV system is operational 24 hours a day, 7 days a week.

The images are transmitted to a video Digital Video Recorder which are housed within a secure, locked communication box. Access to the communication box is restricted. The images are stored on the hard drive of the Digital Video Recorder.

The transmitted images can be viewed live in the front office or on office PC 'OFFICE-03'. The following members of staff have authorisation to access the CCTV footage:

- The headteacher: Gemma Hillier
- The deputy head: Vicki Marshall
- The data protection officer: Nicola Cook

- The system manager (Office staff): Claire Weaver & Charlie Lenton
- Anyone with express permission of the headteacher

The data will be held for 30 days, after this period of time it will be overwritten.

The CCTV system provides school video pictures, which are transmitted from cameras positioned in various locations throughout the school site. All of the CCTV cameras are fixed on a particular scene and do not have audio recording enabled. The cameras are located:

- Facing the playground x2
- Facing the school playing field x2
- Facing the car park
- Facing the footpath from the front entrance
- Facing the EYFS play area
- Inside the School entrance lobby
- Inside the Inclusion Corridor
- Inside Sapphire intervention room
- Inside Emerald intervention room
- Inside the Music room

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

The information is used to ensure the health and safety and security of pupils, staff and visitors. They can be used to detect unauthorised visitors, pupils with poor behavior/internal truancy, and protection of damage to school assets. The information may be shared with the Senior Leadership Team and the Police for investigation and enforcement purposes.

Disclosure of data is covered by the school's internal processes which are fully compliant with UK GDPR laws and relevant legislation and Codes of Practice.

Individuals can request copies of CCTV data which contains their personal information by submitting a subject access request.

Scope

The CCTV data captured is video recordings. By default the CCTV may be picking up special category data

including race/ethnic origin and the health of an individual.

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 system is live, 24 hours a day, 365 days a year. Storage is limited to 30 days, after which the data is deleted.

Context

The school provides education to its students on a term time basis with staff delivering the National Curriculum. The school may receive a number of visitors on a daily basis including contractors, inspectors, support and agency staff, etc. Data stored can affect over 300 people who regularly use the school site, to include but not be limited to:

- Staff
- Pupils
- Visitors
- Peripatetic music staff
- Governors
- Lettings
- Holiday club leaders and children
- Community Payback Team (HMRC)

The CCTV already existed at school so the expectation and acceptance is already there. The addition of the inside CCTV will add to everyone's safety.

The school does inform pupils, staff and visitors that CCTV is in use by installing signs explaining the areas where CCTV monitoring is taking place, along with a contact telephone number.

The CCTV system is capable of identifying individuals from the system and the images can be used in both criminal and civil court cases.

If a Subject Access Request is made data may be downloaded or copied for release to the data subject or a third

party (in the case of a Data Protection request). Each request for data must be requested in line with our Data Protection Policy.

We have no other public concerns. The school has a CCTV Policy. The system is operated in line with relevant legislation and the Surveillance Camera Code of Practice 2022. Staff operating/using the system have undertaken Data Protection training.

Purpose

The aim is to keep staff and children safe, with a positive effect on those concerned. The purposes listed in the above policy give more detail.

Processing will be no different to the old CCTV system so will not be affected.

Consultation Process

A letter will be issued to parents, giving them a 4-week notice period before any additional cameras are switched on. Parents are able to raise any concerns to the headteacher or DPO during this time.

Governors have already been consulted and approved the CCTV.

The CCTV will be maintained by Blue Chip Security.

Necessity & Proportionality

We need to keep all people on site safe, CCTV gives us impactful security. By restricting the access to this as above, the CCTV remains proportionate. It also gives the school the following benefits:

- demonstrates a duty of care to its pupils, staff, and visitors
- protects the fabric of the school both externally and internally
- as a consequence of this budgets can be reduced/deferred to other school projects
- encourages improvement pupil behavior
- provides assistance in the detection and prevention of crime
- to assist in managing the school

The CCTV system is referenced in the school's Privacy Notices.

The lawful basis for processing includes the following:

- Public Task - Article 6 (Lawful Basis) & Reasons of Substantial Public Interest - Article 9 (Lawful Condition) under Data Protection Law
- The Common Law Duty of Care
- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

Cameras are located in areas where pupils and staff have access. Cameras are not located in areas where privacy is expected.

The only way to negate the need for CCTV would be additional staff presence before school, after school and during breaks along with improved lighting. Additional staff would need to act as witnesses during any interventions, meetings and additional staff would need to be employed overnight and at weekends.

The lawful basis for processing is contained in the school's Privacy Notices. Where there have been material changes to the way CCTV is used, the school will undertake a review of its CCTV system to ensure compliance and mitigate against 'function creep.'

We take on subject access requests carefully and appropriately. We restrict the sharing of data to only those authorised on our policy and remain compliant at all times.

Any international transfers of data will be encrypted and password protected.

Identify & Assess Risks

Source of risk and the nature of potential impact on individuals.	**Options to reduce or eliminate risk**	**Likelihood of harm (remote, possible or probable)**	**Severity of harm (minimal, significant or severe)**	**Overall risk (low, medium or high)**
A privacy breach caused by technical issues or human error, where individuals are at risk of discrimination, identity theft, fraud, loss of confidentiality, reputational damage, physical or emotional harm	Correct training and adequate security systems in place.	remote	severe	low
Poor processes or inadequate due	DPO stays current with law.	remote	severe	low

diligence leading to non-compliance with the UK GDPR, resulting in financial or reputational damage to the school	Data breaches reported to DPO.			
Cyber security breach where data is lost, stolen or corrupted.	Appropriate virus guard and secure servers	remote	severe	low
Positioning of CCTV cameras at entrance points to the school and the issue of privacy		remote	minimal	low
Housing of CCTV cameras outside and ingress of water	Use of waterproof enclosures	possible	significant	medium
Ongoing maintenance of CCTV equipment preventing breakdowns, etc	Blue Chip maintaining CCTV system	possible	significant	medium
CCTV policies and procedures not in place leading to inconsistencies, etc	Policies and procedures reviewed regularly with a process in place for refreshing staff knowledge. Induction for new staff.	remote	significant	low
Appropriate CCTV signage in place which conforms to industry standards	Regular spot checks to ensure signage is not removed or damaged	remote	significant	low
Training not undertaken by those using CCTV	Regular training in GDPR and Information Security. Training uptake is monitored to ensure it is undertaken and completed.	remote	significant	low
Noncompliance when upgrading the school's CCTV system	Use CCTV passport to compliance document	remote	significant	low

Sign off

Item	Name	Date
Measures Approved By	Vicki Marshall (Acting Headteacher)	30th March 2025
Residual Risks Approved By	Vicki Marshall (Acting Headteacher)	30th March 2025
DPO Advice Provided	Nicola Cook (Schools DPO)	27th March 2025

Summary Of DPO Advice		
DPO Advice Accepted Or Overruled By		
Comments		
Consultation Responses Will Be Reviewed By	Vicki Marshall (Acting Headteacher) / Claire Weaver (Office Manager)	
Comments		
This DIPA Will Be Kept Under Review By	Gemma Hillier (Headteacher) / Claire Weaver (Office Manager)	To be reviewed in line with policy