



SURVEILLANCE AND CCTV POLICY

At the Willow Learning Trust (WLT) we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance and CCTV systems, which capture moving and still images of people who could be identified.

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.

The purpose of this policy is to regulate the review, management, operation, and use of CCTV across the WLT in accordance with data protection legislation, including the Data Protection Act 1998 and the General Data Protection Regulation (2018).

1. Legal Framework

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

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation (2018)
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information Act 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

This policy operates in conjunction with the individual school child protection/safeguarding policies and the following WLT policies:

- Freedom of Information Policy
- Data Security Policy
- Photography and Videos and School Policy
- GDPR Data Protection Policy
- Data Retention Policy

2. Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video footage will be applicable
- **Overt surveillance** – any use of surveillance for which authority 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 are not informed of such surveillance.

The Willow Learning Trust (WLT) does not condone the use of covert surveillance when monitoring WLT staff, pupils and /or volunteers. Any overt surveillance footage will be clearly signposted around the schools.

3. Roles and responsibilities

The role of the data protection officer (DPO) includes:

- Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that processing of surveillance and CCTV footage is done legally and fairly.
- Ensuring that surveillance and CCTV footage is collected for legitimate reasons and ensuring that it is used accordingly.
- Ensuring that surveillance and CCTV footage collected 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.
- 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
- Monitoring the performance of the WLT's data protection impact assessment (DPIA), and providing advice where requested.
- Reviewing the CCTV Policy to ensure that it is compliant with current legislation.
- Monitoring legislation to ensure the WLT is using surveillance fairly and lawfully.

The role of the CEO, Executive Headteacher (primaries) and Headteachers includes:

- Meeting with site staff 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.
- Communicating any changes to legislation with all members of staff.

The role of the Trust Network Manager (TNM) includes:

- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

4. Purpose and justification

The WLT will only use surveillance cameras for the safety and security of the WLT schools, staff, pupils and visitors. Surveillance will be used as a deterrent for violent behaviour and damage to the schools. The WLT will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in classrooms or any changing facilities.

5. Protocols

The surveillance systems:

- Will be registered with ICO in line with data protection legislation.
- Are closed digital systems which do not record audio.
- Have been designed for maximum effectiveness and efficiency; however the WLT cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.
- Will not be intrusive.

Warning signs have been placed throughout the WLT premises where the surveillance systems are active, as mandated by the ICO's Code of Practice.

6. Security

Access to the surveillance systems, software and data will be strictly limited to authorised operators and will be password protected.

The authorised CCTV systems operators are:

- Executive Headteacher;
- Headteachers, SLT and site staff;
- Trust Network Manager.

The main control facilities are kept secure and locked when not in use. Surveillance and CCTV systems will be tested for security flaws regularly to ensure that they are being properly maintained at all times. Any cameras that present faults will be repaired as to avoid any risk of a data breach. Visual display monitors are displayed on specific, authorised, networked PCs.

7. Privacy by design

The use of surveillance cameras and CCTV will be critically analysed using a DPIA. If the DPIA reveals any potential security risks or other data protection issues, the WLT will ensure they have provisions in place to overcome these issues.

The WLT will ensure that the installation of the surveillance and CCTV systems will always reflect the objectives of this policy. The systems will be designed to take into account effects on individuals and their privacy and personal data. If the use of a surveillance and CCTV system is too privacy intrusive, the WLT will seek alternative provision.

8. Code of practice

- The WLT understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- The WLT notifies all pupils, staff and visitors of the purpose for collecting surveillance data via policies and privacy notices.
- 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 one month for security purposes; the CEO, Executive Headteacher (primaries), Headteachers and the TNM are responsible for keeping the records secure and allowing access.

9. Access

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed. Individuals also have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. For further details about individual's rights and SAR's please refer to our Data Protection Policy.

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.

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 solicitors 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 Headteachers will make the final decision as to whether recorded images may be released to persons other than the police. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example time, date and location. All disks containing images belong to, and remain the property of, the WLT.

As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and the images pixelated so that only the person requesting access can be identified. If it is not possible to conceal the identity of others, disclosure is unlikely. Refusal to disclose images, even if pixelated, may be appropriate where its release is:

- Likely to cause substantial and unwarranted damage to an individual;
- Likely to prejudice the legal rights of individuals or jeopardise an ongoing investigation.

10. Monitoring and review

This policy will be reviewed every 2 years, or in light of any changes to relevant legislation by the DPO and the CEO.

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

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

The scheduled review date for this policy is **May 2023**