SURVEILLANCE & CCTV POLICY

Date of Policy: September 2023

Review Date*: September 2025

Coordinator (s): Mrs Wright, Ms Gregory and Mr Barr

*** Policy Review: Every two years otherwise dictated by the FGB (Full Governing Body) or by changes in legislation.**

Contents

Statement of intent

At Tower College, 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 schools and its members.

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

- We comply with the GDPR, effective 25 May 2018.
- 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.

1. Legal framework

1.1. This policy has due regard to legislation 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
- Data Protection Act 2018
- 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

1.2. This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'
- DfE (2022) 'Protection of biometric data of children in schools and colleges

1.3. This policy operates in conjunction with the following school policies:

- Online Safety Policy
- GDPR Data Protection Policy
- School Security Policy

2. Definitions

2.1. 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 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.

2.2. Tower College 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.

2.3. Any overt surveillance footage will be clearly signposted around the school.

3. Roles and responsibilities

3.1. 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 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 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.

3.2. Tower College as the corporate body, is the data controller. The Principal and governing body of Tower College therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. The SMT deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy The SMT members that are also Safeguarding Team will act as the data controllers.

3.4. 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.

3.5. The role of the Principal includes:

- 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. Purpose and justification

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

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

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

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

5. The data protection principles

5.1. Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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 are inaccurate, having regard to the purposes for which they are processed, are 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 are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

6. Objectives

6.1. 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.

7. Protocols

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

7.2. The surveillance system is a closed digital system.

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

7.4. 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.

7.5. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

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

8. Security

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

8.2. The school's authorised CCTV system operators are:

- Ms Bingley – Principal
- Mrs Wright – Deputy Principal and DSL
- Ms Gregory – Assistant Principal and DDSL
- Mr Barr – Site Manager
- Mr Taylor – Bursar and Onsite Resident

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

8.4. 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.

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

8.6. Surveillance and CCTV systems will not be intrusive.

8.7. The Site Manager and Principal will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders.

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

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

8.10. Visual display monitors are located in the designated area.

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.

9. Privacy by design

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

9.2. A DPIA will be carried out prior to the installation of any surveillance and CCTV system.

9.3. 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.

9.4. 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.

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

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

9.7. 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.

9.8. 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.

9.9. 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

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

10. Monitoring and review

10.1. This policy will be monitored and reviewed every two years by Mrs Wright, Ms Gregory and the Principal and the governing body.

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

10.3. The DSL and DDSL will communicate changes to this policy to all members of staff.

10.4. The scheduled review date for this policy is September 2025.