STROUD HIGH SCHOOL

SURVEILLANCE AND CCTV POLICY

PURPOSE

1. Aims

At Stroud High School, we take our responsibility towards the safety of staff, visitors and students 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 school and ensure that:

- We comply with the UK General Data Protection Regulation (UK GDPR), effective 25 May 2018.
- The images that are captured are useable for the purposes we require them.
- We assure 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 CCTV systems which capture images of people who could be identified.

2. Legal Framework

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 UK General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Student 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

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

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- Information Commissioner's Office (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

This policy operates in conjunction with the following school policies:

- E-security Policy
- Freedom of Information Policy
- UK GDPR Data Protection Policy

3. 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 and audio 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 will not be informed of such surveillance.

Stroud High School does not condone the use of covert surveillance when monitoring the school's staff, students and/or volunteers. Covert surveillance will only be operable in extreme circumstances. Any areas covered by overt surveillance will be clearly signposted.

4. Roles and Responsibilities

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

- Offering advice to the Data Controller regarding processing surveillance and CCTV footage in accordance with data protection legislation.
- Reporting to the highest management level of the school, e.g. the governing board.
- Providing advice where requested regarding Data Protection Impact Assessment for CCTV.

The IT Manager is the Data Controller. The governing body of Stroud High School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The IT Manager deals with day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the Data Controller.

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.
- 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.

The role of the Headteacher includes:

- Making decisions where CCTV is needed to justify its means.
- Seeking appropriate guidance 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, students and visitors in the purpose of:

- for the prevention of crime,
- to protect the school buildings from damage or unauthorised ingress when the buildings are not in use,
- or, to Safeguard pupils and staff while on the school site.

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.

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

6. The Data Protection Principles

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 UK 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.

7. Objectives

The surveillance system will be used to:

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

8. Protocols

The surveillance system is registered with the Information Commissioner's Office (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.

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 trained on individuals 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.

9. Security

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

The school's authorised CCTV system operators are:

- Headteacher
- IT Manager and IT Technicians
- Site Manager

The Headteacher has authorized the following roles to make requests to view CCTV data:

- All members of the Leadership Team
- Key Stage Managers

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

The Headteacher may authorise and document any additional person in the employment of Stroud High School to view CCTV data for a specific event related to an identified purpose of the system.

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 annually to ensure that they are always being properly maintained.

Surveillance and CCTV systems will not be intrusive.

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

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

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

Visual display monitors are located in the designated area.

10. Privacy by Design

The use of surveillance cameras and CCTV will be subject to a Data Protection Impact Assessment (DPIA), in consultation with the DPO.

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

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.

11. 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 students, staff and visitors of the purpose for collecting surveillance data via notice boards, 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 six days 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, students 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, students 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 from 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 through which people can access information and submit complaints.
- 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 students, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

12. Access

This policy comes under the wider Data Protection Policy of the school.[1] Individuals who want to request data access are encouraged to follow the process outlined in that document. The conditions for CCTV do not override those in the overarching policy, other than the retention period for CCTV data is much shorter so any requests falling outside the seven-day period from a specific event will be automatically turned down due to the automatic deletion set out in this policy.

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

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

Individuals 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.

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.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

[1] See https://s3-eu-west-1.amazonaws.com/sh2-stroudhigh-gloucs-sch-uk/media/downloads/dataprotectionpolicy.pdf.

Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher 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 a further two months. 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.

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
- 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.

Date of Policy: October 2023 Next Review: October 2026
Monitored by: Resources Committee