

Surveillance and CCTV Policy

Adopted by the Board of Trustees – April 2018

Reviewed Annually – Latest Review Autumn Term 2026

Contents:

Statement of intent

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Purpose and justification
5. The data protection principles
6. Objectives
7. Protocols
8. Security
9. Privacy by design
10. Code of practice
11. Access
12. Monitoring and review

Statement of intent

At St Margaret's Academy, we take our responsibility towards the safety of staff, visitors, and pupils very seriously. To that end, we use surveillance cameras to deter and monitor any instances of aggression, anti-social behaviour, or physical damage to our school and its community.

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 General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Data (Use and Access) Act 2025 (DUAA).
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured that their personal data is handled strictly 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 or detect a crime
- Using images of individuals that could affect their privacy

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR) (as amended by the Data (Use and Access) Act 2025)
- The Data Protection Act 2018 (DPA 2018)
- The Data (Use and Access) Act 2025 (DUAA)
- The Protection of Freedoms Act 2012
- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- 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
- The Human Rights Act 1998

1.2. This policy has been created with regard to the following statutory and non-statutory guidance (note that under the DUAA 2025, functions of the Information Commissioner's Office (ICO) transition to the Information Commission):

- Home Office (2021) *'Surveillance Camera Code of Practice'*
- Information Commissioner's Office (ICO) *'Guidance on video surveillance (including CCTV)'*
- Information Commissioner's Office (ICO) *'Guide to the UK General Data Protection Regulation (UK GDPR)'*

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

- GDPR Data Protection Policy
- Information Security Policy
- ICO Guidance – *Taking Photos in School*

2. Definitions

2.1. For the purpose of this policy, the following definitions apply in accordance with the Surveillance Camera Code of Practice:

- **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 is applicable.

- **Overt surveillance:** Any use of surveillance that is open, clearly signposted, and for which authorisation does not fall under the Regulation of Investigatory Powers Act 2000.

- **Covert surveillance:** Any use of surveillance which is intentionally hidden from the subjects it is recording, meaning subjects are not informed of such surveillance.

2.2. St Margaret's Academy does not condone the use of covert surveillance when monitoring the school's staff, pupils, visitors, and/or volunteers. Covert surveillance will only ever be considered in extreme, exceptional circumstances where strictly permitted by law and authorised in advance.

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

3. Roles and responsibilities

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

- Advising on Subject Access Requests (SARs) and Freedom of Information (FOI) requests in line with data protection legislation and the Freedom of Information Act 2000.

- Monitoring the school's compliance with data protection legislation when handling and processing surveillance and CCTV footage.

- Advising on legal requirements for obtaining, retaining, and securely destroying surveillance and CCTV footage.

- Ensuring that where consent is relied upon for any related processing, it is clear, positive, and unambiguous (pre-ticked boxes and silence are non-compliant).

- Advising on the maintenance of comprehensive and accurate records of data processing activities (ROPA), including surveillance and CCTV processing.

- Advising on privacy notices so data subjects are informed of how their data captured in CCTV footage will be used, their rights, and the security measures implemented to protect their personal information.

- Preparing reports and management information on the school's level of data protection risk and processing performance, reporting directly to the highest management level (the Board of Trustees).

- Abiding by statutory confidentiality requirements in relation to duties undertaken while in the role.

- Monitoring the performance of the school's Data Protection Impact Assessments (DPIAs) and providing specialist advice where requested.

3.2. St Margaret's Academy, as the corporate body (Academy Trust), is the **Data Controller**. The Board of Trustees therefore holds overall legal responsibility for ensuring that records are maintained, including security, governance, and access arrangements in accordance with statutory regulations.

3.3. The **Headteacher** deals with day-to-day operational matters relating to data protection and acts as the **designated operational Data Protection Lead** on behalf of the Academy Trust.

3.4. On behalf of the Data Controller, the designated operational staff ensure that:

- Surveillance and CCTV footage is processed lawfully, fairly, and transparently.
- Surveillance and CCTV footage is collected only for specified, legitimate reasons and is not used incompatibly with those purposes.
- Surveillance and CCTV footage is adequate, relevant, and not excessive in relation to the purpose for which it is collected.
- Any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Footage containing personal data is protected against accidental or unlawful destruction, loss, alteration, and unauthorised disclosure, particularly when transmitted or stored over networks.

3.5. The role of the **Headteacher** includes:

- Meeting with the DPO and School Business Manager to decide where CCTV is needed and ensuring its use is justified and proportionate.
- Conferring with the DPO regarding the lawful processing and disclosure of surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy annually to ensure it remains compliant with current legislation.
- Monitoring legislative changes to ensure the school uses surveillance fairly and lawfully, and communicating updates to 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 against violent or aggressive behaviour, theft, and physical damage to the school premises.

4.3. Under no circumstances will surveillance or CCTV cameras be installed in school classrooms, toilets, or any changing facilities.

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

4.5. Lawful basis for processing
Under Article 6 of the UK GDPR (as amended by the Data (Use and Access) Act 2025), St Margaret's Academy relies on the following lawful bases to operate its surveillance and CCTV system:

- **Public Task (Article 6(1)(e)):** Processing is necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested in the Academy Trust—specifically our statutory duty to safeguard and promote the welfare of pupils and maintain a safe learning environment.

- **Recognised Legitimate Interests (Article 6(1)(ea)):** Where processing falls outside our core public task (such as out-of-hours site perimeter monitoring and asset protection), processing is necessary for recognised legitimate interests as defined

under the Data (Use and Access) Act 2025—specifically the prevention and detection of crime, ensuring public safety, and safeguarding vulnerable individuals.

5. The data protection principles

5.1. Personal 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 incompatible with those purposes (further processing for archiving in the public interest, scientific or historical research, or statistical purposes is not considered incompatible where appropriate safeguards apply).
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that inaccurate personal data 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. Objectives

6.1. The surveillance system will be used to:

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

7. Protocols

7.1. The Academy Trust will maintain its data protection registration with the Information Commission (formerly the ICO) in line with statutory requirements.

7.2. The surveillance system is a closed digital system which **does not record audio**.

7.3. Clear warning signs are placed throughout the premises where the surveillance system is active, in accordance with the Surveillance Camera Code of Practice and ICO/Information Commission guidance.

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. Cameras will not be actively trained on specific individuals unless an immediate response to a live safety or security incident is required.

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

8. Security

8.1. Access to the surveillance system, software, and recorded data is strictly limited to authorised operators and is protected by strong passwords and access controls.

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

- **Nikki O'Dwyer** – Headteacher
- **Onewest** – Data Protection Officer (DPO)
- **Karen Colmer** – CCTV System Controller
- **Nicole Turner** – System Administrator
- **Sound and Visual** – External CCTV Maintainer (operating under a written data processing agreement)

8.3. The main control facility and recording hardware are kept secure and locked when not in use.

8.4. Surveillance and CCTV systems will be tested for security flaws and operational integrity annually to ensure they are properly maintained at all times.

8.5. Surveillance and CCTV systems will be positioned and operated so as not to be unnecessarily intrusive.

8.6. The Headteacher and School Business Manager determine recording schedules (such as continuous recording outside school hours to deter intruders). Any unnecessary or expired footage is automatically overwritten or securely deleted from the school system.

8.7. Any cameras or system components that present faults will be repaired promptly to prevent any risk of a security vulnerability or personal data breach.

8.8. Visual display monitors are located in the front office and the back office, positioned so they cannot be viewed by unauthorised visitors or passers-by.

9. Privacy by design

9.1. The use of surveillance cameras and CCTV is critically analysed using a Data Protection Impact Assessment (DPIA), in consultation with the DPO.

9.2. A DPIA will be carried out prior to the installation of any new surveillance or CCTV system, or before making significant changes to existing camera locations or capabilities.

9.3. If a DPIA reveals potential security risks or data protection issues, the school will implement appropriate technical and organisational measures to mitigate those risks before deployment.

9.4. Where the school identifies a high risk to individuals' rights and freedoms that cannot be mitigated, the school will consult the Information Commission before operating the CCTV system and will act upon its advice.

9.5. The school will ensure that the installation and continued operation of surveillance and CCTV systems remain necessary and proportionate to their stated purpose.

9.6. If the use of surveillance or CCTV in a particular area is deemed too privacy-intrusive, the school will seek less intrusive alternatives.

10. Code of practice

10.1. The school recognises that recording images of identifiable individuals constitutes processing personal data and must be carried out strictly in accordance with data protection legislation.

10.2. The school notifies all pupils, staff, parents, and visitors of the purpose for collecting surveillance data via prominent signage, privacy notices on the school website, letters, and emails.

10.3. CCTV cameras are only placed where they do not intrude on reasonable expectations of privacy and where they are necessary to fulfil their security and safeguarding purpose.

10.4. All surveillance footage will be kept for a **maximum of six weeks** for security purposes unless isolated and retained securely in connection with a specific incident, safeguarding investigation, legal claim, or Subject Access Request. The Headteacher and School Business Manager are responsible for keeping retained records secure and controlling access.

10.5. The school operates its surveillance system solely for the prevention and detection of crime and the promotion of the health, safety, and welfare of staff, pupils, and visitors.

10.6. The surveillance and CCTV system is owned by St Margaret's Academy, and images from the system are strictly controlled and viewed by authorised personnel only.

10.7. The school ensures that its surveillance and CCTV system creates a safer environment for staff, pupils, and visitors and operates consistently with all statutory obligations. This policy is published on the school's website.

10.8. The surveillance and CCTV system will:

- Be designed and operated to take into account its effect on individuals, their privacy, and their personal data.
- Be transparent and provide clear contact points (the School Business Manager and the DPO) through which individuals can request information or submit complaints.
- Maintain clear responsibility and accountability procedures for all images and information collected, held, and used.
- Operate under defined policies and procedures communicated across the school community.
- Retain images and information only for as long as strictly required.
- Restrict access to retained images and information with clear rules on who can view or extract footage.
- Meet all relevant operational, technical, and competency standards in accordance with the law.
- Be protected by stringent physical and cyber security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure policies and technical standards are maintained.

- Be used solely for its intended purposes, including supporting safety, protecting pupils, staff, and visitors, and assisting law enforcement.

- Be accurate, calibrated (including accurate time and date stamps), and well maintained.

10.9. Data protection complaints
In accordance with the Data (Use and Access) Act 2025, any individual who has concerns about how St Margaret's Academy collects, uses, stores, or discloses their personal data via its surveillance and CCTV system has the right to submit a formal complaint directly to the Academy before escalating the matter to the regulator:

- **How to complain:** Complaints can be submitted in writing or electronically to the School Business Manager or the Data Protection Officer (Onewest) using the contact details published on the Academy's website and Privacy Notice.

- **Acknowledgement:** The Academy will acknowledge receipt of a data protection complaint within **30 days** of receiving it.

- **Investigation and outcome:** The Academy will take appropriate steps to investigate the complaint without undue delay, keep the complainant informed of progress, and provide a written outcome explaining any actions taken.

- **Escalation to the regulator:** If the complainant remains dissatisfied after receiving the Academy's final response, they have the right to escalate their complaint to the Information Commission (formerly the Information Commissioner's Office).

11. Access and Subject Access Requests (SARs)

11.1. Under the UK GDPR, individuals have the right to obtain confirmation as to whether their personal data is being processed and to request access to that data.

11.2. All recording media, storage drives, and exported files containing images remain the property of St Margaret's Academy.

11.3. Individuals have the right to submit a Subject Access Request (SAR) to access personal data captured of them on CCTV.

11.4. The school will verify the identity of the person making the request (and, where relevant, parental responsibility or authority to act on a pupil's behalf) before any information is supplied.

11.5. A copy of the requested personal data will be supplied free of charge; however, the school may charge a reasonable administrative fee for additional copies of the same information.

11.6. Where an SAR is made electronically, the information will be provided in a commonly used electronic format unless the individual requests otherwise.

11.7. Requests by external parties for viewing or obtaining digital recordings will be assessed by the Headteacher, in consultation with the DPO, on a case-by-case basis with close regard to data protection and Freedom of Information legislation.

11.8. Where a request is manifestly unfounded, excessive, or repetitive, the school may charge a reasonable fee based on the administrative cost of providing the information, or refuse to act on the request.

11.9. All SARs will be responded to without undue delay and at the latest within **one calendar month** of receipt, unless the response timeframe is paused or extended in accordance with statutory rules.

11.10. Where the school reasonably requires additional information to verify the requester's identity, or to clarify the scope of the request so that specific CCTV footage can be located (such as the date, approximate time, and location on site), the school will **pause ("stop the clock" on) the one-month response period** from the date clarification is requested until the necessary information is received.

11.11. Searches for personal data within CCTV recordings will be limited to what is **reasonable and proportionate** in the context of the request.

11.12. In the event of numerous or complex requests, the period of compliance may be extended by up to a further **two months**. The individual will be informed of this extension, along with an explanation of why it is necessary, within one month of receipt of the request.

11.13. Where a request is manifestly unfounded or excessive and the school decides to refuse it, the individual will be informed within one month of receipt of the decision, the reasons for it, and their right to submit a direct complaint to the Academy, complain to the Information Commission, and seek a judicial remedy.

11.14. Access to and disclosure of recorded CCTV images is strictly controlled to protect the privacy rights of third parties and to preserve the evidential chain of custody should footage be required for legal or police proceedings.

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

- **The police:** Where the images recorded would assist in a specific criminal inquiry or safeguarding investigation.

- **Prosecution agencies:** Such as the Crown Prosecution Service (CPS).
- **Relevant legal representatives:** Such as solicitors and barristers acting in legal proceedings.

- **Data subjects (or their authorised representatives):** Where disclosure is required under data protection legislation. When processing SARs for CCTV footage, the Academy may redact/blur third parties or provide a series of still images where necessary to protect the rights and freedoms of other identifiable individuals.

- **Freedom of Information applicants:** Only where non-personal information (such as policy documents or camera statistics) is disclosable under the Freedom of Information Act 2000.

11.16. All requests for access or third-party disclosure will be logged, and the Headteacher (in consultation with the DPO) will make the final decision regarding release to parties other than the police.

12. Monitoring and review

12.1. This policy will be monitored and reviewed on an annual basis by the Headteacher, the School Business Manager, and the DPO, and approved by the Board of Trustees.

12.2. The Headteacher and School Business Manager, supported by the DPO, are responsible for monitoring legislative and regulatory changes that may affect this policy and updating it accordingly.

12.3. The Headteacher will communicate any updates to this policy to all members of staff.

12.4. Date for next review: September 2027