The Aspire Educational Trust

Surveillance and CCTV Policy

Contents:

Statement of intent

At the Aspire Educational Trust, 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 school and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems on trust sites 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

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
- 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 (2013) 'The Surveillance Camera Code of Practice'
- ICO (2017) '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'

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

- Photographic and Video Images Policy
- E-safety Policy
- Freedom of Information and Publication scheme.
- Data Protection 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. 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.

2.2. The Aspire Educational Trust does not condone the use of covert surveillance when monitoring the trust and its schools 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:

- Supporting the trust and its schools with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.
- Reviewing the trust's Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the trust and its schools are using surveillance fairly and lawfully.
- Ensuring that all data controllers at the trust and its schools 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.
- Monitoring the trust and its schools keep 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.
- Monitoring data subjects are informed of how their data is captured in surveillance and CCTV footage, will be used by the trust and its schools, their rights for the data to be destroyed and the measures implemented by the trust and its schools to protect individuals' personal information.
- Preparing reports and management information on the trust's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the trust.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the trust and its schools' data protection impact assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing across the trust to senior leaders and the board of trustees.

3.2. The Aspire Educational Trust, as the corporate body, is the overall data controller. The Board of Trustees of The Aspire Educational Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. The principal in each of the trust's schools deals with the matters relating to data protection in their school and thus, for the benefit of this policy will act as the joint data controller with the trust.

3.4. The role of the data controller in each school 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:

- Meeting with the DPO to monitor where CCTV is needed and to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Communicating any changes to policy and legislation with all members of staff.

4. Purpose and justification

4.1. The trust and its schools 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 trust's schools.

4.3. The trust and its schools 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 facility.

4.4. If the surveillance and CCTV systems fulfil their purpose and are no longer required the trust and its schools 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.

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. Surveillance systems will be registered with the ICO in line with data protection legislation.

7.2. Warning signs will be placed throughout the trust premises where surveillance systems are active, as mandated by the ICO's Code of Practice.

7.3. Surveillance systems have been designed for maximum effectiveness and efficiency; however, the trust and its schools cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

7.4. Surveillance systems will not be trained on individuals unless an immediate response to an incident is required.

7.5. Surveillance systems will not be trained on private vehicles or property outside the perimeter of the school.

8. Security

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

8.2. Each trust school's authorised CCTV system operators are identified and given authorisation to access the system. The positions of those named as authorised system operators should be:

- The principal or their deputy in their absence.
- The trust's CEO
- The trust's DPO.
- The school's data controller (the principal).
- The trust's Facilities Manager
- The school's CCTV data processor – Site Maintenance Officer and bursar/School Business Manager

8.3. An up-to-date log will be maintained for each surveillance and CCTV system detailing who accesses the data, when and for what purpose.

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

8.5. 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.

8.6. Surveillance and CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times.

8.7. Surveillance and CCTV systems will not be intrusive.

8.8. The principal will decide when to record footage on their site, e.g. a continuous loop outside the school grounds to deter intruders.

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

8.10. Systems will have a separate audio and visual system, if required, that can be run independently of one another. Audio CCTV will only be used in the case of deterring aggressive or inappropriate behaviour.

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

8.12. Visual display monitors are located in the secure areas where they can not be viewed by unauthorised personnel which would present a data breach.

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 trust and its schools will ensure they have provisions in place to overcome these issues.

9.4. Where the trust and its schools identify a high risk to an individual's interests, and it cannot be overcome, the trust will consult the ICO before they use CCTV, and the trust and its schools will act on the ICO's advice.

9.5. The trust and its schools 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 trust and its schools will seek alternative provision.

10. Code of practice

10.1. The trust and its schools understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

10.2. The trust and its schools notify all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

10.3. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

10.4. All surveillance footage will be kept for no longer than six months for security purposes. Footage will be overwritten in a timeframe to meet the needs of the individual site and its system. The retention period will be recorded on the individual school's data asset register. The principal is responsible for keeping the records secure and allowing access.

10.5. The trust and its schools have surveillance systems for the purpose of 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 systems are owned by individual schools and images from the system are strictly controlled and monitored by authorised personnel only.

10.7. The trust and its schools will ensure that their surveillance and CCTV systems are used to create a safer environment for staff, pupils and visitors to trust premises, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

10.8. The surveillance and CCTV systems on trust premises will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point, the DPO, 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 trust.
- 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 pupils, staff and volunteers, and law enforcement.

10.9. Be accurate and well maintained to ensure information is up-to-date.

11. Access

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

11.2. All disks containing images belong to, and remain the property of, the trust and its schools.

11.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

11.4. The trust and its schools will verify the identity of the person making the request before any information is supplied.

11.5. A copy of the information will be supplied to the individual free of charge; however, the trust and its schools may impose a 'reasonable fee' to comply with requests for further copies of the same information.

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

11.7. Requests by persons outside the trust for viewing or copying disks, or obtaining digital recordings, will be assessed by the principal, who will consult 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, a reasonable fee will be charged.

11.9. All fees will be based on the administrative cost of providing the information.

11.10. All requests will be responded to without delay and at the latest, within one month of receipt.

11.11. 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.

11.12. Where a request is manifestly unfounded or excessive, the trust 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.

11.13. In the event that a large quantity of information is being processed about an individual, the trust will ask the individual to specify the information the request is in relation to.

11.14. 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.

11.15. 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

11.16. 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.

12. Monitoring and review

12.1. This policy will be monitored and reviewed on an annual basis by the DPO.

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

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

12.4. The scheduled review date for this policy is Spring 2021.