Surveillance and CCTV Policy

Key Document Details:			
Author:	Data Protection Officer	**Department:**	Central Services
Reviewer:	Head of Primary Education	**Version No:**	1.2
Last Review:	September 2023	**Next Review:**	September 2025
Approver:	Executive Team	**Date Ratified:**	September 2023

Contents

Document Change History

Date:	Version:	Description of Changes:
08/22	1.1	Addition of biometric data legislation.
09/23	1.2	Reviewed and amended authorised CCTV operators.

Mission Statement

"To nurture and develop all people in our Trust so that they reach their full potential academically, vocationally, and personally, including being positive role models for future generations in the community. We will achieve this by providing high quality values-based education that cultivates employability and life skills making our schools the first choice for young people, parents, carers, staff and employers."

Values

The values of Respect, Excellence, Collaboration, Independence, Perseverance, Enjoyment, Leadership, Integrity and Care are central to everything we do at the Skills for Life Trust.

Statement of Equality

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Purpose

At Skills for Life 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 Trust and its members.

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

- We comply with the UK 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 UK General Data Protection Regulation (UK GDPR)
- The 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
- 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) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- 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 Trust policies:

- Data Protection Policy
- Data Security Policy
- E-Safety Policy

- Freedom of Information
- Records Management Policy
- Subject Access Request Procedure

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. Skills for Life Trust does not condone the use of covert surveillance when monitoring the Trust'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 Trust.

3. Roles and responsibilities

3.1. The role of the data protection officer (DPO) is to ensure that measures are in place for:

- 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 Trust 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 (where required) is clear, positive and unambiguous
- 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 Trust, their rights for the data to be destroyed and the measures implemented by the Trust to protect individuals' personal information
- Monitoring the performance of the Trust's data protection impact assessment (DPIA)

and providing advice as requested
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation
- Monitoring legislation to ensure the Trust is using surveillance fairly and lawfully
- Communicating any changes to legislation with all members of staff

3.2. Skills for Life Trust, as the corporate body, is the data controller. The Trust therefore have overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. 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
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period
- Ensuring that the processing of any biometric data, including any processing carried out by a third party on their behalf complies with the Data Protection Act 2018, UK GDPR and Protection of Freedoms Act 2012.
- Identifying the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented.
- Ensuring that the processing of biometric data is done so in line with the school's Protection of Biometric Data Policy

3.4. The role of the Headteacher at individual trust schools includes:

- Meeting with the DPO, Trust IT Network Manager and Facilities Manager to:
    - Decide where CCTV is needed
    - Justify its means
    - Identify the lawful bases for processing

4. Purpose and justification

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

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

4.3. Audio recording is only permitted in reception areas to ensure the safety of office staff.

4.4. CCTV systems may only be used to actively monitor communal areas, via a live feed, to ensure the safety of staff and students.

4.5. CCTV systems will not be used to actively monitor staff while teaching.

4.6. If the surveillance and CCTV systems fulfil their purpose and are no longer required the Trust 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 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.

6. Privacy by design

6.1. A DPIA will be carried out prior to the installation of any new, or additions to a surveillance and CCTV system.

6.2. If the DPIA reveals any potential security risks or other data protection issues, the Trust will ensure they have provisions in place to overcome these issues.

6.3. Where the Trust identifies 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 will act on the ICO's advice.

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

6.5. If the use of a surveillance and CCTV system is too intrusive, the Trust will seek alternative provision.

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 Trust 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 Trust.

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 Trust's authorised CCTV system operators are:

- CEO
- Head of Primary Education
- IT Team

- Data Protection Officer
- Trust Facilities Manager

8.3. The authorised CCTV system operators at each school are:

- Headteacher
- Senior Leadership Team
- Heads of Year (Secondary)
- Site Manager

8.4. An access log will show each operator's most recent login.

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

8.6. 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.

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

8.8. Surveillance and CCTV systems will not be intrusive.

8.9. The Headteacher and Trust Facilities Manager will decide when to record footage, e.g. a continuous loop outside the Trust grounds to deter intruders.

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

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

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

9. Code of practice

9.1. The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

9.2. The Trust notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

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

9.4. All surveillance footage will be kept for 28 days.

9.5. The Headteacher, Trust Facilities Manager and Trust IT Network Manager are responsible for keeping the records secure and allowing access.

9.6. The Trust 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, pupils and visitors.

9.7. The surveillance and CCTV system is owned by the Trust and images from the system are strictly controlled and monitored by authorised personnel only.

9.8. The Trust will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the Trust, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

9.9. 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, academy offices, through which people can request access to information and submit complaints. Requests and complaints will then be directed to the DPO and data protection coordinator
- 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
- Be accurate and well maintained to ensure information is up-to-date.

9.10. To comply with the requirements of the Protection of Freedoms Act 2012, the school will notify all parents of its intention to process pupils' biometric data, and emphasise that parents may object at any time to the processing of the information.

9.11. The Trust will ensure that pupils' biometric data is not taken or used as part of a biometric recognition system.

10. Access

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

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

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

10.4. The Trust will verify the identity of the person making the request before any information is supplied.

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

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

10.7. Requests by persons outside the Trust for viewing or copying disks, or obtaining digital recordings, will be assessed by the data protection coordinator, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

10.8. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

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

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

10.11. 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.

10.12. 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.

10.13. 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.

10.14. 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.

10.15. 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

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