DANES EDUCATIONAL TRUST

SURVEILLANCE AND CCTV PROCEDURE [Elstree Screen Arts]

RESPONSIBILITIES	
To determine and approve policy and ensure compliance	CEO
To implement, deliver and comply	Headteacher
APPROVAL DATE	Summer Term 2023
COMMITTEE	N/A
DURATION	1 Years
REVIEW DATE	Summer Term 2024
SLT LEAD	Chief Operating Officer
Equality Impact Assessment	As part of the review process, this procedure has been subject to an Equality Impact Assessment

CONTENTS

STATEMENT OF INTENT

At Danes Educational Trust, we take our responsibility towards the safety of staff, visitors and learners 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 at the school and ensure that:

- We comply with the Data Protection Act 2018, incorporating the UK General Data Protection Regulations (GDPR), effective 25 May 2018.
- The images that are captured are usable 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 all relevant legislation and statutory guidance 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
- 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) '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'

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

- Data Protection Including Biometrics Policy
- Data security Procedure
- Data Retention Procedure
- Freedom of Information Publication Scheme 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. 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. Danes Educational Trust does not condone the use of covert surveillance when monitoring the school's governors, staff, learners and/or volunteers. Covert surveillance will only be operable in extreme circumstances for example a legal obligation or where this has been requested by the police to assist in a criminal investigation

3. ROLES AND RESPONSIBILITIES

3.1. The role of the school 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 UK 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 trust 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 trust board.
- Ensuring the Security of the system and that the protocols and code of practice are followed.

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

3.3. The school DPO deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller for the individual Trust school.

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 Headteacher includes:

- Meeting with the school DPO to decide where CCTV is needed to justify its means.
- Conferring with the school 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 systems as a deterrent and for the safety and security of the school and its staff, learners 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 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.

5. THE DATA PROTECTION PRINCIPLES

5.1. Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with the following purposes ; further processing for archiving data in the public interest, scientific or historical research, statistical 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. 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 learners, staff, Governors, Trustees 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 which does not record audio.

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:

- Mr Chris Mitchell - Principal
- Ms Adele Wallis – Data Protection Officer
- Ms Nikki Ward – Assistant Principal & Safeguarding Lead
- Mr Kyle Warusevitane – Network Administrator
- Mr Patrick Kane – Caretaker
- Ms Clare Buckle – Pastoral Support Manager & Deputy Safeguarding Lead

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 by the schools data protection officer.

8.5. Surveillance and CCTV systems will be tested once a month to ensure that they are operational.

8.6. Surveillance and CCTV systems will not be intrusive.

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

8.8. Any unnecessary footage captured by the school CCTV system will be securely and automatically deleted after a set period of time, typically between 14 and 45 days depending on the capabilities of the CCTV system.

8.9. Where a school has a separate audio and visual system, these must be run independently of the CCTV system.

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

8.11. Access to CCTV images are via IP address and/or locally installed software/applications that will be provided to the authorised members of staff detailed in this policy.

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.

10. CODE OF PRACTICE

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

10.2. The school notifies all learners, staff, Governors, Trustees and visitors of the purpose for collecting surveillance data via signage and privacy notices.

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 on the surveillance system will be kept for a maximum of two months for security purposes however this could be less dependent on the storage capabilities of the individual school's hardware; the headteacher and the data controller are responsible for keeping the records secure and allowing access.

10.5. 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, learners and visitors.

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

10.7. The school will ensure that the surveillance and CCTV system is used to maintain a safe environment for Governors, Trustees, staff, learners and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The Data Protection Including Biometrics Policy is available from the Trust's website.

10.8. 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, the school 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 school.
- Only keep images and information for as long as legally 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 learners, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

11. ACCESS

11.1. Under the UK 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 school.

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 school 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 school 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 school for viewing or copying disks, or obtaining digital recordings, will be assessed by the headteacher, 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 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.

11.13. 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.

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. Under section 7 of the Data Protection Act 2018 and the UK GDPR, individuals who are the subject of personal data are entitled to request access to it. This includes CCTV images where they are defined as personal data within the meaning of the Act. If a request is received, a copy of the images must be provided within 1 calendar month of the request

11.16. There are occasions when CCTV footage will not be considered individual personal data. This would be when CCTV footage shows more than one individual, for example when viewing a playground area or locker facility. In this instance the school would not be permitted to release the footage under GDPR legislation.

11.17. 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:

- Parents/carers - where the images recorded would assist in highlighting a specific incident including; violent behaviour, damage to the school and putting at risk the safety and security of the school and its staff, learners and visitors. In these circumstances parents/carers will be allowed to view the relevant excerpts of the recorded images on the school premises under the supervision of a member of the senior leadership team. The parents/carers (and their representatives where appropriate) will not have access to the excerpts through links or emails. The excerpts may only be viewed in person on the school premises. Where possible, the school should ensure that the identity of other individuals in the recorded images is protected through the use of software to obscure the other individuals. In circumstances where that is not possible e.g. recorded images of a playground with multiple individuals the member of the senior leadership team must not disclose the names or any other personal identifiable data of the individuals captured in the recording and Parents/carers are required to sign a non-disclosure agreement (appendix 1) confirming that they will not disclose the identity of any other individuals captured in the recorded images to third parties. The non-disclosure agreement is to be held on file by the school DPO
- 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

11.18. 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.

12. MONITORING AND REVIEW

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

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

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

Appendix 1

VIEWING OF CCTV RECORDED IMAGES NON-DISCLOSURE AGREEMENT

Name of parent/carer	
Name of child	
Year group	
Date of incident	
Description of incident and recorded images viewed	
Date the recorded images were viewed on the school premises	
Statement of non-disclosure	**I confirm that I have viewed recorded images of the incident under the supervision of the authorised CCTV system operator.** **I acknowledge that there were multiple individuals captured on the recorded image and confirm that I will not disclose the identity or personal data of any other individuals captured in the recorded image to any third party.**
Signed by parent/carer	
Name of member of SLT	
Declaration of member of SLT	**I confirm that the recorded images of the incident were shown to the parent/carer on the school premises.** **Before allowing the recorded images to be shown the images of other individuals captured in the recorded images have been obscured** **Where there are multiple individuals captured in the recorded images and it has not been possible to obscure their identity I have not disclosed any other personal identifiable data of the individuals.**
Signed by SLT	
This signed agreement is to be held on file by the School Data Protection Officer	