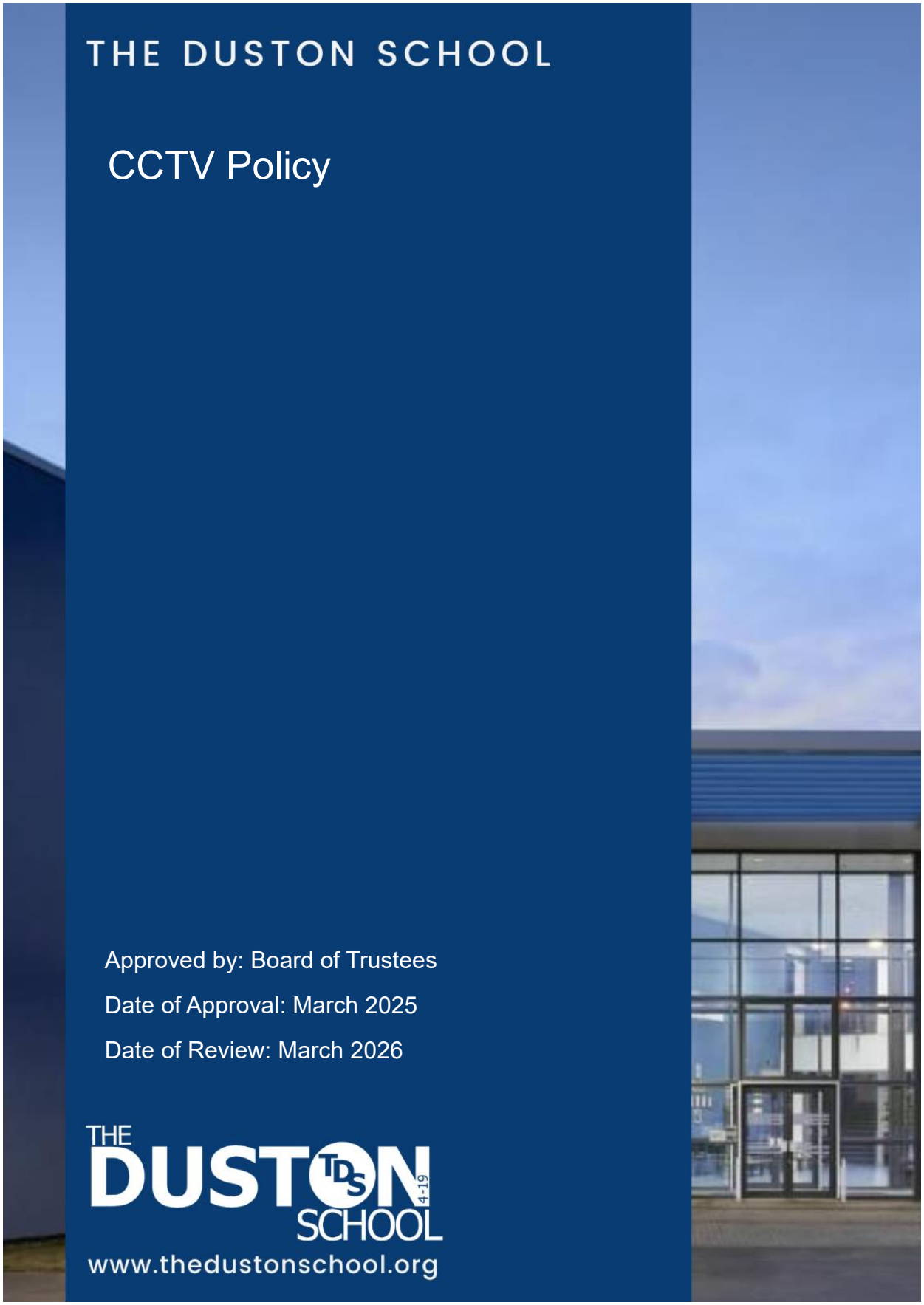

THE DUSTON SCHOOL

CCTV Policy

Approved by: Board of Trustees

Date of Approval: March 2025

Date of Review: March 2026

THE DUSTON SCHOOL 4-19

www.thedustonschool.org

Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defence of any litigation proceedings
- The CCTV system will not be used to:
- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency\safeguarding\investigation incident occurring.
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

Relevant legislation and guidance

This policy is based on:

Legislation

UK General Data Protection Regulation

Data Protection Act 2018

Human Rights Act 1998

European Convention on Human Rights

The Regulation of Investigatory Powers Act 2000

The Protection of Freedoms Act 2012

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

Guidance

Surveillance Camera Code of Practice (2021)

Definitions

DPO – Data Protection Officer

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed, the proper authorisation forms from the Home Office will be completed and retained.

Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Cameras are located in all areas of the school premises including but not restricted to:

Air locks

Corridors

Stairs

Fire exits

Outside of toilets but not inside

External communal areas such as the tennis courts and quad

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

Identifies the school as the operator of the CCTV system

Identifies the school as the data controller

Provides contact details for the school

Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

Roles and Responsibilities

The Trustees

The Trustees have the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

The IT Manager

The IT Manager will:

Take responsibility for all day-to-day management of the CCTV system

Attend spot checks by the DPO to ensure that the system is used as agreed

Ensure all persons with authorisation to access the CCTV system and footage have received proper training in the use of the system and will ensure that the 'terms of usage' (appendix 1) has been signed.

Oversee the security of the CCTV system and footage

Check the system for faults and security flaws termly

Ensure the data and time stamps are accurate termly

The Data Lead

The school's DPO will:

Ensure that the guidance set out in this policy is followed by all staff

Review the CCTV policy to check that the school is compliant with legislation

Train all staff to recognise a subject access request

Deal with subject access requests in line with the Freedom of Information Act (2000)

Monitor compliance with UK data protection law

Advise on and assist the school with carrying out data protection impact assessments

Act as a point of contact for communications from the Information Commissioner's Office

Ensure data is handled in accordance with data protection legislation

Ensure footage is obtained in a legal, fair and transparent manner

Ensure footage is destroyed when it falls out of the retention period

Keep accurate records of all data processing activities and make the records public on request

Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information

Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified

Ensure that the CCTV system is not infringing on any individual’s reasonable right to privacy in public spaces

Carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period

Receive and consider requests for third-party access to CCTV footage

In consultation with the IT Manager, decide whether to comply with disclosure of footage requests from third parties.

Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is capable of recording audio but is not enabled in all areas.

IT Services will monitor the system to ensure uptime is kept at a maximum, If there are any issues IT services are to be contacted.

Storage of CCTV Footage

Footage will be retained for 30 days, any footage that is used within an 'incident' will be kept for an indefinite period.

Recordings may be downloaded for evidence purposes.

Access to CCTV footage

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in this document, or if there is a lawful reason to access the footage.

All access to data is automatically audited by the system with usernames and timestamps.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

Staff access

The following members of staff have authorisation to access the CCTV footage:

Organisation Admin

IT Manager
ICT Technician
Chief Financial Manager

Full Access - To view all cameras, and able to export, share and see incidents

Senior Vice Principal – Head of KS4
Vice Principal – Head of KS3
Vice Principal for Safeguarding and attendance
Educational Support Administrator

Access to all cameras, and Air detectors - View only

Senior Leadership Team
HR manager
Head's PA
Directors of Year
Assistant Directors of Year
Lead Practitioners

CCTV footage will only be accessed from authorised personnel's work devices
All users will sign an agreement to acknowledge that all access and actions are audited within the software and will be subject to spot checks each term to ensure it is being used correctly.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

Subject access requests (SAR)

According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the request, the school will immediately issue a receipt and will then respond within a calendar month. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

All staff have received training to recognise SARs. When a SAR is received staff should inform the school's data protection representative or DPO in writing. When making a request, individuals should provide the school with reasonable information such as the date, time, and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in this document (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the headteacher and the school's designated data protection representative or DPO.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The school's designated data protection representative and DPO will consider very carefully how much footage to disclose and seek legal advice if necessary.

The school's data protection representative / DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the school's designated data protection representative / DPO.

Data protection impact assessment (DPIA)

The school follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including the replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims.

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by Andy Clarke

Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be done annually and/or whenever cameras are moved, and/or new cameras are installed.

If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

Security

The system manager will be responsible for overseeing the security of the CCTV system and footage

The system will be constantly monitored for faults.

Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure to IT services.

Footage will be stored securely and encrypted wherever possible, It is preferred to keep recordings within the platform provided.

Proper cyber security measures will be put in place to protect the footage from cyber attacks

Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

Complaints

Complaints should be directed to the headteacher and should be made according to the school's complaints policy.

Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

Links to other policies

Data protection policy

Privacy notices for parents, pupils, staff & governors

Safeguarding policy

Appendix 1

Form for Access request. (Verkada TDS CCTV System)

Name

Position

Date

Access level requested

I agree to use the CCTV system for professional use only, and comply with the guidelines stated in this document.

I understand that all actions and use linked to my user account is audited within the system and may be spot checked from time to time.

Signature