THE TWO COUNTIES TRUST

CCTV POLICY

Date of issue: 06/11/2023

1. Purpose

1.1 The purpose of this CCTV Policy is to regulate the management, operation and use of the CCTV systems (Closed Circuit Television) at The Two Counties Trust and its schools, hereafter collectively referred to as 'the Trust'.

1.2 The Trust's CCTV systems will be used to record footage 24 hours a day, 365 days a year (either continuously or on motion), the purpose being to:

- Help make students, staff, visitors and other members of the Trusts communities feel safe.
- Protect members of the Trust community from harm to themselves or to their property.
- Deter criminality in the Trust .
- Protect the Trust's assets and buildings.
- Assist the police to deter and detect crime.
- Determine the cause of accidents and incidents.
- Assist in the effective resolution of any disputes which may arise in the course of employee or student proceedings.
- To assist in the defence of any litigation proceedings.

1.3 The Trusts 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 incident occurring.
- Pursue any other purposes than the ones stated above.
- Record audio.

1.4 The list of uses of CCTV is not exhaustive and other purposes may become relevant according to the circumstances.

2. Scope

2.1 This policy covers all CCTV cameras and recording devices in the Trust, as well as everyone affected by the use of CCTV including staff, students, contractors, visitors, volunteers and families.

2.2 The Trust has a current Data Protection Registration Certificate issued by the Information Commissioner's Office as required under the terms of the Data Protection Act 2018. The systems comply with the requirements of the Data Protection Act 2018 and UK GDPR and the ICO CCTV checklist which can be found here.

2.3 Footage or any information obtained through the Trust CCTV systems will never be used for commercial purposes.

2.4 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, approved by the Data Protection Officer and only for the purposes of assisting in the investigation of a specific crime.

2.5 Operators and those with responsibility for our CCTV systems should refer to this policy to understand the objectives of the systems, and responsibilities of those involved in its operation and management and to restrict unauthorised persons from gaining access to recorded images.

3. Policy Principles

3.1 Legislation & Guidance

The CCTV Policy includes the requirements of the current legislation and guidance relating to the use of CCTV, which comprise principally of:

- 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
- Surveillance Camera Code of Practice (2021) (Guidance)

Specifically, the Data Protection Act 2018 relates to data processing of all types. The definition of data under the Act is "Personal data" means any information relating to an identified or identifiable living individual. It requires the person to be identified by a number of means, which can include photographic or video footage.

The definition of Processing is much wider in its scope. "Processing", in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as:

- Collection, recording, organisation, structuring or storage.
- Adaptation or alteration.
- Retrieval, consultation or use.
- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Restriction, erasure or destruction.

Data in the case of CCTV recordings is in the form of recorded images of individuals that can be identified from these images.

Having regard for these definitions, it is recognised that the use of CCTV for surveillance purposes is encompassed by the requirements of the Data Protection Act.

3.2 Definitions

For clarity and to avoid any ambiguity, the following definitions are provided which covers any use of such wording in this CCTV policy.

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.

3.3 ICO Registration

The Two Counties Trust's registration number with the Information Commissioners office is Z7196664.

4. Policy Elements

4.1 CCTV Signage

CCTV signage is erected around all of our buildings, within prominent locations which clearly identifies that CCTV recording is in operation. For details of the location and type of signage required please refer to Appendix 1.

4.2 Location of recording equipment

Recording and processing equipment are located in a secured lockable enclosure accessible only to authorised persons.

The Trust will ensure cameras are only located in places that require monitoring in order to achieve the aims of the CCTV system.

Cameras are not, and will not, be aimed off school grounds into public spaces or people's private property, nor will they be located within private spaces such as toilets and changing rooms.

Cameras will not be positioned in classrooms with the exception of agreed use for professional development opportunities and if excessive vandalism occurs.

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

Please refer to school specific site plans for the locations of cameras.

4.3 System Management & Responsibilities

There are several key contacts at each school who hold responsibility for the management of each CCTV system. The table below sets out the different roles and authorities involved in the CCTV management; schools must nominate and disclose a System Manager.

Role/Authority	Responsibilities
Trust Board	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 3.1) is complied with.
Headteacher	The Headteacher will: • Familiarise themselves with this CCTV policy. • Take responsibility for all day-to-day leadership and management of CCTV as set out in this policy. • Liaise with the Trust, and if required, the Data Protection Officer, to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified. • Ensure that the guidance set out in this policy is communicated to and followed by school staff. • Sign off on any expansion or upgrading to the CCTV system, after having taken advice from relevant professionals and taken into account the result of a data protection impact assessment. • Decide, in consultation with relevant professionals, whether to comply with disclosure of footage requests from third parties.
ICT Support Team	The ICT Support Team will: • Manage the day-to-day maintenance and operation of the CCTV system. • Oversee the security of the CCTV system and footage. • Check the system for faults and security flaws regularly. • Ensure the data and time stamps are accurate regularly. • Administrate the CCTV system, • Ensure that only those with authority to view images can do so and for a specific, legitimate purpose. • Check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional. • Train colleagues with authorisation to access the CCTV system and footage in the use of the system and in data protection. • Apply software and security updates published by the equipment's manufacturer as soon as possible on receipt.

	• Ensure faults in the system are repaired as soon as possible, according to the proper procedure • Ensure sufficient security is in place to protect the CCTV system and footage from cyber attacks • Carry out monthly checks which confirm that footage is being stored accurately, and being deleted after the retention period. • Conduct data protection impact assessments with assistance from the DPO and other professionals as required. • Ensure footage is destroyed when it falls out of the retention period. • Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals captured 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.
Data Protection Officer (DPO)	The DPO: • Monitors the Trust's compliance with UK data protection law. • Advises and assists the Trust with carrying out data protection impact assessments. • Acts as a point of contact for communications from the Information Commissioner's Office. • Advises on and ensures that the Trust is handling data in accordance with data protection legislation and that footage is obtained in a legal, fair and transparent manner. • Advises on requests received for third-party access to CCTV footage. • Supports with subject access requests requiring CCTV.

4.4 Storage of and access of footage

Access to CCTV footage

Access will only be given to authorised persons for the purpose of pursuing the aims stated in section 1 of this policy, or if there is a lawful reason to access the footage.

Any individuals that access the footage must do so with their own named account, so that this is recorded in the CCTV systems access log.

The following members of staff have authorisation to access and review footage on their school CCTV system:

- The Headteacher.
- Senior Leadership Team.
- DSL, Deputy DSL and Safeguarding Officers.
- Pastoral Staff (for behaviour issues).
- The Head of ICT and members of the ICT team.
- Members of the Trust Executive Team.
- Members of the Trust Board and relevant school Local Governing Body.
- The Data Protection Officer.
- Anyone with express permission of the Headteacher and / or the Head of ICT.

CCTV footage will only be accessed from authorised personnel's work devices, and CCTV system software will be installed accordingly to facilitate this, or from designated CCTV monitors where individuals do not have a work device.

All designated CCTV monitors will be positioned so only authorised personnel can view the footage.

All members of staff who have access will be provided a demonstration of the system by the ICT support team when access is issued, to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be subject to an investigation which may lead to disciplinary action, and in certain circumstances unlawfully viewing footage may constitute a criminal offence.

Download, storage and sharing of CCTV footage

In order to maintain and preserve the integrity of the data (and to ensure admissibility in any legal proceedings) any downloaded footage from the CCTV system must be prepared, stored and shared in accordance with the following procedures.

- Footage downloaded from the system should contain a watermark with time and date.
- When storing footage on digital media (i.e. on the network or cloud), it should be saved in a location which is secure and only accessible to members of staff who have authorisation, as detailed above.
- When storing on physical media, media must be cleaned of any previous recording before use and kept secure at all times.
- When a member of staff requests footage they must specify what the incident was, at what time, and where.
- Downloaded footage released because there is satisfactory evidence for a secure legal basis must be sealed, witnessed and signed, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.
- If downloaded footage is archived the reference must be noted.
- When footage is being shared, it will be done so securely with encryption and/or password protection.
- Images may be viewed by the police for the prevention and detection of crime.
- A record will be maintained of the release of any downloaded footage.
- Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded footage remains the property of the school, and are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded footage to any other person.
- The police may require the school to retain the downloaded footage for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.
- Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Boards, Legal department.

Retention of CCTV footage

The retention period for live recording will be set to 30 days on each CCTV system, with new footage automatically overwriting older footage which has reached this age.

When specific footage is required and downloaded from the CCTV system, the retention period of this will be determined on a case by case basis.

On occasion footage may need to be retained for a longer period of time, for example where there is an ongoing investigation into a safeguarding or employment issue, or a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

4.5 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.

We are also able to rely on an exemption of the Data Protection Act which states that personal data processed for reasons of prevention and detection of crime and apprehension and prosecution of offenders are exempt, providing that the following criteria are met:

- We have assessed that if we had to inform individuals that recording was taking place it would prejudice our objective.
- We have reasonable cause to suspect specific criminal activity or actions that could result in a serious breach of staff or volunteer behaviour expectations is taking place.
- That covert processing is only carried out for a limited and reasonable period of time and relates to the specific suspected criminal activity.

4.6 Subject Access Requests

According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves by making a Subject Access request. Please refer to the Trust's Subject Access Request Protocol for further information.

4.7 Third party access

It will not be common practice to release CCTV footage unless satisfactory evidence for a secure legal basis can be provided. This is authorised within Section 115, Crime and Disorder Act 1998.

In such cases, CCTV footage will only be shared with an external third party to further the aims of the CCTV system set out in section 1 (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. LADO, investigators).

All requests for access should be set out in writing and sent to the headteacher and Head of ICT or a member of the Trust's Executive team.

The Trust will comply with any court orders that grant access to the CCTV footage. The Trust will provide the courts with the footage they need without giving unrestricted access. The DPO will provide advice on how much footage to disclose.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR. All disclosures will be recorded by the Trust.

4.8 Data protection impact assessment (DPIA)

The Trust 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 (stated in section 1).

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 the System Manager.

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.

If any security risks are identified in the course of the DPIA, the Trust will address them at the earliest opportunity.

5. General Data Protection Regulation

5.1 All data within this policy will be processed in line with the requirements and protections set out in the UK General Data Protection Regulation and the Data Protection Act 2018.

Appendix 1: CCTV Signage

It is a requirement of the General Data Protection Regulation (GDPR) to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded.

To ensure the Trust is GDPR compliant, will use signage at prominent points around our school buildings. This signage must state the reason for the usage of CCTV as per point 1 in this policy. A summary of this purpose on signage, such as "24 hour CCTV is in operation at this school for the safety of children, staff and visitors and for the purpose of crime prevention", is sufficient.

In the case of the Trust and its schools, it is clear that we are the operators of the CCTV system for the purpose defined above, and therefore signage does not need to specify who the operator is.

Examples of compliant signage:

Examples of non-compliant signage (unless used in conjunction with compliant signage):