We are an ambitious and inclusive Trust of schools
strengthening communities through excellent education.

Management of Information - CCTV Policy

Responsibility for approval: Senior Executive
Approval date March 26

Contents Page

Table of Contents

1.0 Policy Statement

1.1 We are an ambitious and inclusive Trust of schools strengthening our communities through excellent education. We are committed to providing excellent education for every child, every day, and aim to strengthen and work with our communities to ensure confident compliance.

2.0 Scope and Purpose

2.1 The school recognises that CCTV systems can be privacy intrusive.

2.2 For this reason, the Trust has carried out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below.

2.3 The result of the data protection impact assessment has informed the Trust's use of CCTV and the contents of this policy.

2.4 Review of this policy shall be repeated regularly and whenever new equipment is introduced, a review will be conducted, and a risk assessment put in place. We aim to conduct reviews no later than every two years.

2.5 The purpose of the CCTV system is to assist the school in reaching the following objectives:

- To protect pupils, staff and visitors against harm to their person and/or property;
- To increase a sense of personal safety and reduce the fear of crime;
- To protect the school buildings and assets;
- To support the police in preventing and detecting crime;
- To assist in identifying, apprehending and prosecuting offenders;
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence; and
- To assist in managing the school.

2.6 The purpose of this policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the school. Each School will have a proforma containing the CCTV system used by the school in the reception area which comprises of:

Camera Type	Location	Sound	Recording Capacity	Swivel/Fixed
		Y/N	Y/N	S/F

CCTV cameras are in areas where individuals would have an expectation of privacy. These are in toilets, open-space bathrooms and changing facilities. We have carried out a Data Protection Impact Assessment (DPIA) to assess the risks and have consulted parents prior to installing them in these areas.

3.0 Definition

3.1 For the purpose of this document the Ted Wragg Multi Academy Trust is referenced to as the Ted Wragg Trust or TWT or the Trust and applies to both the Trust and our Trust of School. Amend all definitions dependant on audience of policy.

4.0 Legal Framework

4.1 This Policy is a Trust wide Policy and will be published on both the Trust and School websites and will be included in the Trust's Policy Monitoring Schedule. It forms part of our Management of Information Suite.

5.0 Statement of Intent

5.1 CCTV cameras are installed in such a way that they are not hidden from view. Signs are predominantly displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

5.2 The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

5.3 The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

5.4 The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

5.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

5.6 Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

5.7 The planning and design have endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

5.8 Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

5.9 Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

5.10 CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. **Data storage is automatically overwritten by the system after a period of one month**.

5.11 Recorded images will only be retained long enough for any incident to come to light (e.g., for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 6 months.

6.0 System Management

6.1 Access to the CCTV system and data shall be password protected and will be kept in a secure area.

6.2 The CCTV system will be administered and managed by the school who will have appointed a System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager, the system will be managed by the Compliance Lead.

6.3 The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.

6.4 The CCTV system is designed to be in operation during the school day and information of these hours can be found at the school. The school does not guarantee that it will be working during these hours.

6.5 The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

6.6 Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

6.7 Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

6.8 Where a person other than those mentioned above, requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused.

6.9 Details of all visits and visitors will be recorded in a system log book including time/data of access and details of images viewed and the purpose for so doing

6.10 The school operates an **internally managed CCTV system** within the school grounds and buildings. This system is managed by the school and access is restricted to the Compliance Lead and staff, as determined by the Headteacher. Access is strictly controlled in line with this policy.

6.11 For PFI schools the **external CCTV system**, covering the school grounds, is managed by **Pinnacle**, the building owner's appointed on-site facilities provider. Pinnacle is the **data controller** for the external CCTV system in PFI schools and is responsible for its operation, maintenance and security of the captured data.

6.12 In PFI schools the school does not have routine access to the external CCTV system. Where internal staff require access—for example, to investigate an incident on school grounds—a formal request will be made to Pinnacle in accordance with their procedures.

6.13 In PFI schools all requests for access to external CCTV footage must be made to Pinnacle directly or alternatively they can also be routed via the school's **Compliance Lead**, who will liaise directly with Pinnacle on your behalf.

7.0 Downloading Captured Data on to Other Media

7.1 In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures: -

- Each downloaded media must be identified by a unique mark.
- Before use, each downloaded media must be cleaned of any previous recording.
- The System Manager will register the date and time of downloaded media insertion, including its reference.
- Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, 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 media is archived, the reference must be noted.
- If downloaded media is put onto a device, the device will be encrypted, and password protected.

7.2 Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may

be used as evidence, it shall be preferable, if possible, for that person to withhold viewing of the data until asked to do so by the police.

7.3 A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

7.4 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 media (and any images contained thereon) remains the property of the school and downloaded media (and any images contained thereon) 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 media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

7.5 The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

7.6 Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the school's Compliance Lead and a decision made by a senior leader of the school in consultation with the school's Data Protection Officer.

8.0Requests for Access by the Data Subject

8.1 The Data Protection Act provides data subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the Compliance Lead for the School.

8.2 Please refer to our Data Protection Policy with Subject Access Request appendix for further details.

8.3 If we cannot comply with the request, the reasons for not being able to comply will be documented and the data subject will be advised of these in writing.

8.4 The assigned manager responsible for the CCTV system will liaise with the Data Protection Officer, Judicium Consulting, and the school's Designated Safeguarding Lead to determine whether disclosure of the images will reveal third-party information, to assess the risks involved with disclosure and the reasonableness in disclosure.

8.5 Particular care should be exercised when images of other people are included in the materials for disclosure. Images of other individuals will, if possible, be redacted unless there would be an expectation that their images would be released in such circumstances. Non-disclosure will be appropriate in most circumstances. If there is any doubt about what information must be provided to enquirers, please contact the school's Data Protection Officer, Judicium Consulting.

8.6 **For PFI schools t**he school is **not the data controller** for external CCTV images captured on school grounds. SARs or other rights requests relating to the external CCTV system cannot be fulfilled by the school.

8.7 In PFI schools any SAR relating to external CCTV footage will be acknowledged by the school and then redirected to **Pinnacle**, who are responsible for responding as the data controller.

8.8 The school will support Pinnacle, where appropriate, in identifying the time and nature of the incident to assist their search for footage.

8.9

9.0 Complaints About the Use of CCTV

9.1 Any complaints in relation to the school's CCTV system should be addressed to the Headteacher.

10.0 Public Information

10.1 A proforma to summarise the type of CCTV and where this is located can be found at the school site in reception. This will also contain details of the System Manager and hours of operation.