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

CCTV Policy

Responsibility for approval: Senior Executive
Date of Approval : November 2026
Next review: October to December 2027

Contents Page

1.0 Policy Statement
2.0 Scope and Purpose
3.0 Definition
4.0 Legal Framework
5.0 Statement of Intent
6.0 System Management
7.0 Downloading Captured Data on to Other Media
8.0 Requests for Access by the Data Subject
9.0 Complaints About the Use of CCTV
10.0 Public Information

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. 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 the cause of accidents and other adverse incidents and prevent recurrence; and
- To assist in managing the school.

2.6 The purpose of this policy is to regulate the management, operation and use of CCTV systems at Trust schools. Each school will maintain a local proforma, available in reception, summarising the CCTV systems in use.

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

2.7 Where CCTV cameras are installed in areas where individuals would have an expectation of privacy, including toilets, open-space bathrooms or changing facilities, the school will have completed a DPIA and consulted parents before installation.

3.0 Definition

3.1 For the purpose of this policy, Ted Wragg Multi Academy Trust is referred to as Ted Wragg Trust, TWT or the Trust. This policy applies to the Trust and all Trust schools.

4.0 Legal Framework

4.1 This is a Trust-wide policy and will be published on the Trust and school websites and included in the Trust Policy Monitoring Schedule. It forms part of the Data Protection Policy Page.

5.0 Statement of Intent

5.1 CCTV cameras are installed in such a way that they are not hidden from view. We do not covertly record anyone. Signs are displayed where relevant so that staff, pupils, visitors and members of the

public are made aware that they are entering an area covered by CCTV. The signs contain contact details and a statement of the purposes for which CCTV is used.

5.2 The CCTV system will seek to comply with the requirements of the Data Protection Act 2018 and the most recent Information Commission guidance.

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 of 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 entertainment purposes.

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

5.8 Warning signs will be clearly visible on the site and will make clear who is responsible for the equipment.

5.9 Where wireless communication takes place between cameras and a receiver, signals will 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 an incident to come to light and 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 six months.

6.0 System Management

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

6.2 The CCTV system will be administered and managed by the school, which will appoint a System Manager responsible for restricting access in accordance with the principles and objectives expressed in this policy. In the absence of the System Manager, the system will be managed by the Compliance Lead.

6.3 The system and the data collected will only be available to the System Manager, their 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. Information about the operating hours can be found at the school. The school does not guarantee that the system will be working during these hours.

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

6.6 Cameras have been selected and positioned to best achieve the objectives set out in this policy, in particular by providing clear, usable images. Images must be as clear as possible so that they are effective. To achieve this, the school will ensure that:

- equipment is properly installed, serviced, checked and maintained, with maintenance logs retained;
- any recording media is of good quality and replaced if image quality begins to deteriorate;

- where the time and date are recorded, the equipment is set accurately and checked and documented regularly;
- cameras are correctly positioned;
- assessments are made as to whether constant real-time recording is necessary or recording can be limited to times when suspect activity is likely to occur;
- cameras are protected from vandalism so far as possible; and
- where cameras break down or are damaged, the school arranges timely repair.

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 Powers Act 2000.

6.8 Where a person other than those authorised requests access to CCTV data or the system, the System Manager must satisfy themselves of the identity and legitimacy of purpose of the person making the request. Where doubt exists, access will be refused.

6.9 Details of all visits and visitors will be recorded in a system logbook, including the time and date of access, details of images viewed and the purpose for doing so.

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 onsite facilities provider. Pinnacle is the data controller for the external CCTV system in PFI schools and is responsible for its operation, maintenance and the security of 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 its procedures.

6.13 In PFI schools, all requests for access to external CCTV footage must be made to Pinnacle directly. Alternatively, they may be routed through the school's Compliance Lead, who will liaise with Pinnacle.

7.0 Downloading Captured Data on to Other Media

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

- Each downloaded item must be identified by a unique mark.
- Before use, each downloaded item must be cleaned of any previous recording.
- The System Manager will register the date and time of insertion, including its reference.
- Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, dated and stored in a separate secure evidence store. If a copy was not made for the police before sealing, a copy may be made later provided that the media is resealed, witnessed, signed, dated and returned to the evidence store.
- If downloaded media is archived, its reference must be recorded.
- If downloaded media is placed on 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 System Manager, their replacement, the Headteacher and other authorised senior leaders. Where one of these people may later be called as a witness and the content may be used as evidence, it is preferable, where possible, for that person not to view 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 Where images are required as evidence, a copy may be released to the police under the procedures described in this policy. The footage remains the property of the school and must be treated in accordance with data protection legislation. The school retains the right to refuse permission for the police to pass the footage to another person. Where a court requires release, the media will be produced from the secure evidence store in its sealed bag.

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

7.6 Applications from outside bodies, including solicitors or parents, to view or release images will be referred to the school's Compliance Lead. A senior leader will make the decision in consultation with the Trust's Data Protection Officer.

8.0 Requests for Access by the Data Subject

8.1 The Data Protection Act 2018 provides data subjects whose image has been captured by the CCTV system and who can be identified with a right to access personal data held about them, including CCTV images. Requests should be made to the school's Compliance Lead.

8.2 Please refer to the Trust Data Protection Policy, including the Subject Access Request appendix, for further details.

8.3 If the Trust or school cannot comply with a request, the reasons will be documented and the data subject advised in writing.

8.4 The 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 would reveal third-party information, assess the risks and consider whether disclosure is reasonable.

8.5 Particular care must be exercised where images of other people are included. Images of other individuals will, where possible, be redacted unless there is an expectation that their images would be released in the circumstances. Non-disclosure will be appropriate in most circumstances. Where there is doubt, advice should be sought from the Data Protection Officer.

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

8.7 Any subject access request relating to external CCTV footage at a PFI school will be acknowledged by the school and redirected to Pinnacle, which is responsible for responding as data controller.

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

9.0 Complaints About the Use of CCTV

9.1 Complaints and enquiries about the operation of CCTV systems should be raised under the Trust Data Protection Policy. They should be sent to the Trust Lead for Complaints and Compliance at dataprotection@tedwraggtrust.co.uk.

9.2 If a member of staff believes that there has been a personal data breach or another breach of legal obligations, they must report it urgently in accordance with the data breach reporting process set out on the Data Protection Policy Page.

10.0 Public Information

10.1 A proforma summarising the type and location of CCTV in use at each school will be available at the school reception. It will also contain details of the System Manager and operating hours.

10.2 Copies of this policy will be available to the public through the Trust and school websites.

Document Review and Approval

- Policy owner: Trust Lead for Complaints and Compliance.
- Responsibility for approval: Senior Executive.
- Review cycle: Annual.