

Sir Henry Fermor C of E Primary School

CCTV Policy

Approval Arrangements

All statutory policies in the Trust are ultimately the responsibility of the Trust Board. To enable it to discharge this responsibility appropriately and in collaboration with the constituent schools, the Trust Board will either

1. set a full Trust wide policy which applies in the same way to all schools
2. require individual schools to set a policy (in most cases with Trust-provided guidance) appropriate to the needs and circumstances of an individual school

This is a Level 2 Policy against the Trust Governance Plan.

Approval Body:	Headteacher
Author:	Data Protection Officer
Date Approved:	July 2025
Next review:	July 2028
Review Period:	3 years
Version:	2.0

This policy was approved by the Headteacher and the Trust's Data Protection Officer for implementation on the date above and supersedes any previous CCTV policy

Introduction

The vision of the Tenax Schools Trust is to achieve excellence by working together so that all may feel loved and empowered to serve a thriving society. We are committed to education providing life changing transformative opportunities.

Sir Henry Fermor C of E Primary School uses closed circuit television (CCTV) images to reduce crime and monitor its school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to school property.

The system comprises 8 cameras. The CCTV system is operated and monitored by the Site Manager.

Data Protection

The use of CCTV, and the associated images and any sound recordings, is covered by the Data Protection Act.

The school will follow the Information Commissioner's Office (ICO) guidance on CCTV and video surveillance to help ensure it is used responsibly and safeguards both trust and confidence in its continued use. The guidance is published at:

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/about-this-guidance/>

It is a requirement of the UK GDPR and Data Protection Act (DPA) 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school will ensure that this requirement is fulfilled.

Siting the Cameras

Cameras are sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the DPA 2018.

The school has positioned cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

Members of staff have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

Signs are placed so that students, staff and the public are aware that they are entering a zone which is covered by surveillance equipment.

The purpose of the use of CCTV is displayed – e.g. "CCTV in operation for your safety and security"

Storage and Retention of CCTV images

Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded. Recordings are retained for 30 days unless required for evidential value.

All retained data is stored securely at the school, and access to recorded images is restricted to those staff authorised to view them, and will not be made more widely available.

A documented procedure should be kept by the Site Manager which ensures that the accuracy of the system features are checked and if necessary amended or altered.

The Site Manager is responsible for ensuring the following checks are carried out:

To be done daily

- Check all footage is playable
- Check that the cameras and equipment are working properly
- Check that we can retrieve video
- Ensure any special features are accurate (e.g. time display)
- Report immediately if equipment is faulty or damaged via email to SLT

Check that any saved footage is not older than 30 days. If it is it needs to be deleted off of the system.

Subject Access Requests (SAR)

Individuals have the right to request access to CCTV footage relating to themselves under the DPA.

All requests should be made in writing to the Headteacher, Chief Operating Officer or Chief Executive Officer. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example, date, time and location.

The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an investigation.

Access to and Disclosure of Images to Third Parties

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

Requests should be made in writing to the Headteacher, Chief Operating Officer or Chief Executive Officer.

The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

A list of approved staff that have access to CCTV footage is included here as Appendix. This is a stacked system of access level.

It is required that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of data and against accidental loss, damage or destruction. The nature of the data to be processed should be considered and where it contains details of inappropriate/unnecessary material it must be processed with greater care.

Complaints

Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher or the Trust's Data Protection Officer (DPO).

Appendix 1: STAFF ACCESS RIGHTS

Level	Name	Access
1	Site Manager	Full Access & Operational Use
2	SLT	Full Access
3	WLT	Viewing of CCTV footage
5	Office Team	Viewing of CCTV footage
6	All other staff members	Viewing of CCTV footage, provided authorised by Level 2 or above