

Appendix 5 - CCTV Policy

The Trust recognises that CCTV systems can be privacy intrusive.

Objectives

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.

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

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

Purpose of This Policy

The purpose of this policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the Trust.

Statement of Intent

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.

The CCTV system will seek to comply with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 (DUAA), and the most recent Information Commission's Code of Practice.

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

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

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

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.

The system is intended to 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.

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

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

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 no longer than 90 days.

Routine CCTV data storage is automatically overwritten by the system after a period of no longer than 90 days. However, where an incident is identified (such as a security breach, property damage, or a matter likely to lead to disciplinary action), the relevant specific footage will be extracted from the main system and securely stored as a separate record. In accordance with the 'Destruction of Records' provisions in the Trust's Data Retention Policy, this extracted footage will be retained for as long as is necessary to resolve any subsequent formal investigation, data protection complaint, grievance, or legal/tribunal proceedings.

System Management

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

The CCTV system in each school is the responsibility of the Headteacher. The Headteacher may designate a system manager to take day to day responsibility for managing the CCTV system in accordance with the principles and objectives expressed in this policy.

The system will only be available to appropriate members of staff as determined by the Headteacher. The Trust's ICT team and the external CCTV contractor will have the necessary access to support the operation of the system.

The CCTV system is designed to be in operation at all times, though the Trust does not guarantee that it will be working during these hours.

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.

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.

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.

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.

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.

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 Trust and

downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The Trust also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person.

The police may require the Trust 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.

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

Complaints About the Use of CCTV

Any complaints regarding the Trust's processing of personal data via the CCTV system will be handled in accordance with the statutory Data Protection Complaints procedure outlined in the main Data Protection Policy.

Requests for Access by the Data Subject

Data protection legislation (including the UK GDPR and the Data (Use and Access) Act 2025) 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 in accordance with the procedures and statutory deadlines set out in Appendix 1 – Subject Access Requests.