CCTV Policy

Document Title	CCTV Policy
Author	K Thomlinson, GDPR Lead – Central Team
Version Number	Version 1
Approved by	TPT Audit and Risk Committee
Effective from	April 2024
Due for Revision	April 2026

Document Control Table

Document History			
Version	**Date**	**Author**	**Note of Revisions**
V1	April 2024	K Thomlinson	First Trust-wide CCTV policy.

Contents

Introduction

The Prospect Trust (the Trust) recognises that closed-circuit television (CCTV) systems can be privacy intrusive, therefore this policy aims to regulate the management, operation and use of CCTV on Trust property.

The purpose of the CCTV system is to:

- Make members of the Trust community feel safe
- Protect members of the Trust community from harm to themselves or to their property
- Deter criminality in the Trust
- Protect Trust assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defence of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

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, and only to assist in the investigation of a specific crime.

Statement of Intent

CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant so that staff, learners, 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.

Where the CCTV system has audio recording functionality this will be disabled. Where it is not possible to disable the audio function, signs will be put in place to alert people that audio recording is active.

The CCTV system will seek to comply with the requirements both of the Data Protection Act (the Act) and the most recent Commissioner'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. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

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

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.

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, Recorded images will only be retained long enough for any incident to come to light 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 30 days.

Location of Cameras

The Academy Head/Principal will ensure that cameras have been positioned so as to best achieve the objectives set out in this policy. In positioning cameras the Academy Head/Principal will consider proportionately i.e. that the privacy issues arising from the use of a camera can be justified because the camera will resolve a specific issue. The Academy Head/Principal will also ensure that the camera is focused on a relevant space.

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.

System Access

Access to the CCTV system and data shall be password protected and will be kept in a secure area. The Head of Network Services will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy.

The system and the data collected will only be available to the Systems Manager, and appropriate members of staff as determined by the Academy Head/Principal.

Where a person other than those mentioned above, requests access to the CCTV data or system, the Academy Principal/Head must satisfy themselves of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused. Details of all viewings will be recorded in a system log book including time/data of access and details of images viewed and the purpose for so doing.

System Management and Operation

The CCTV system is designed to be in operation 24 hours each day, every day of the year, 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. The System Manager will inform the relevant Site Manager is physical maintenance is required.

Downloading Captured Data on to Other Media

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 stored so that it can be easily identified.
- 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 Academy Principal/Head, 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.

Images may be viewed by the police for the prevention and detection of crime and by the Academy Principal/Head, the Designated Safeguarding Lead and other authorised staff. 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. This may be the case where the staff member has witnessed the incident first-hand.

The Academy will maintain a record of the viewing or release of any downloaded media to the police or other authorised applicants.

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. 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.

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 school's Data Protection Officer and a decision made by a senior leader of the academy in consultation with the Trust's Data Protection Officer. The Academy Head/Principal will keep the CEO and the COO informed and updated on any such requests.

Complaints About the Use of CCTV

Any complaints in relation to the academy's CCTV system should be addressed to Academy Principal/Head.

Subject Access Requests (SARs)

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. SARs should be made, preferably in writing, to the relevant GDPR Lead:

- Frimley CofE Junior School: Clare Wright, Headteacher: info@frimley.surrey.sch.uk
- Tomlinscote School: Rob Major, Principal: rmajor@tomlinscoteschool.com
- Sixth Form College Farnborough: Nicola Mullan, Executive Office Manager: executive_office@farnborough.ac.uk

Requests to view footage will be denied where such viewing would infringe the data protection of others. The Trust will seek advice from the Data Protection Officer when a SAR is received. The Trust employs the services of Judicium Consulting Ltd to act as Data Protection Officer.

Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

Summary of Responsibilities

- Overall responsibility for CCTV: Academy Head/Principal
- Deciding camera locations: Academy Head/Principal
- Determining who has access to footage: Academy Head/Principal
- Enabling the access restrictions: IT
- Installation, removal, physical maintenance: Estates
- Maintenance of the operating system: IT
- Signage: Estates
- Policy Updates: GDPR Lead – Central Team
- Subject Access Requests: Relevant GDPR Lead
- Complaints: Academy Head/Principal

Related Policies

- *Data Protection Policy*
- *Complaints Policy*

These policies can be found on the Trust website.

Policy Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust.