CCTV policy

Authored by:	Deputy Chief Operating Officer	**Date:**	4 November 2021
Last reviewed on:	10 November 2023		
Approved by:	Board of Trustees – 18 October 2022		
Next review due by:	January 2025 (by Board of Trustees)		

1 Introduction

1.1 The Gosforth Federated Academies Limited (Gosforth Group) recognises that CCTV systems can be privacy intrusive.

1.2 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 Objectives

2.1 The purpose of the CCTV system is to assist the trust in reaching these objectives:

(a) To protect and safeguard students, staff and visitors against harm to their person and/ or property;
(b) To assure health and safety requirements are being met;
(c) To increase a sense of personal safety and reduce the fear of crime;
(d) To protect the school buildings and assets;
(e) To support the police in preventing and detecting crime;
(f) To assist in identifying, apprehending and prosecuting offenders;
(g) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence;
(h) To assist in managing schools.

3 Purpose

3.1 The purpose of this policy is to regulate the management, operation and use of the CCTV systems (closed circuit television) across the trust's schools. An inventory of the CCTV systems used by the trust is retained by the Director of Estates and Facilities.

3.2 CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

3.3 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.

4 Statement of intent

4.1 Registration with the Information Commissioner's Office is completed on an annual basis in March of each year.

4.2 The CCTV system will seek to comply with the requirements both of the Data Protection Act 2018 and the most recent Commissioner's Code of Practice.

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

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

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

4.6 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.

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

4.8 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.

4.9 Where wireless communication takes place between cameras and a receiver, it is a requirement that signals shall be encrypted to prevent interception. Gosforth Group does not operate wireless cameras.

4.10 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 28 days.

4.11 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 compelling a need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than is required.

5 System Management

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

5.2 The CCTV systems are administered and managed on a local basis by the school Facilities Manager at each site.

5.3 The following staff are permitted to view and download CCTV footage at each academy, specifically in relation to matters concerning student behaviour, welfare and safeguarding:

- Academy Principal
- Members of the academy senior leadership team
- Academy reception staff
- Academy designated safeguarding leads (DSLs)
- Facilities Managers

5.4 The Trust also has four designated CCTV Systems Managers who take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. The Systems Managers are:

- Chief Operating Officer
- Deputy Chief Operating Officer
- Director of Estates and Facilities
- Deputy Director of Estates and Facilities

5.5 Systems Managers have the authority to view and download CCTV footage appropriate to the purposes set out in section 2.1. The data collected will only be available to the Systems Managers.

5.6 The CCTV systems are 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.

5.7 The Systems Managers will check and confirm the efficiency of the system regularly and that the equipment is properly recording and that cameras are functional.

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

5.9 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.

5.10 Where a person other than those above, requests access to the CCTV data or system, the Systems 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.

5.11 Details of all requests will be recorded in a system logbook including time/ data of access and details of images viewed and the purpose for so doing.

6 Downloading captured data onto other media

6.1 In order to maintain and preserve the integrity of the data (and to ensure its 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:

(a) Each downloaded media must be identified by a unique mark;
(b) Before use, each downloaded media must be cleaned of any previous recording;
(c) Details of any viewed and downloaded CCTV footage will be registered; including the date and time of downloaded media and the reason for viewing and/ or downloading;
(d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the Systems 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 Systems Manager, then dated and returned to the evidence store;
(e) If downloaded media is archived the reference must be noted;
(f) If downloaded media is put onto a device, the device will be encrypted and password protected.

6.2 Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/ her replacement and the Principal 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.

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

6.4 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 trust, and downloaded media (and any images contained thereon) are to be treated in accordance with data protection legislation.

6.5 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.

6.6 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 they are needed by the police.

6.7 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 relevant school in consultation with the trust's DPO.

7 Complaints about the use of CCTV

7.1 Any complaints in relation to a school's CCTV system should be addressed to the relevant Academy Principal.

8 Request for access by the data subject

8.1 The Data Protection Act 2018 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.

8.2 Requests for such data should be made to the trust's Data Protection Officer at dataservices@judicium.com, or by writing to the Data Protection Officer, Judicium Consulting Limited, 72 Cannon Street, London, EC4N 6AE