

Hope SENTAMU LEARNING TRUST

THE COMPASS ACADEMY CCTV POLICY

(in conjunction with the Hope Sentamu Learning Trust's Data Protection Policy (GDPR),
Subject Access Request Policy and Procedures, Health and Safety Policy and
the Trust's Complaints Procedure)

THIS POLICY APPLIES TO ALL HOPE SENTAMU LEARNING TRUST SCHOOLS/ACADEMIES

Document Management:

Date Policy Prepared: February 2018

Date Amended: June 2022

Date Policy Approved: 04 July 2022

Next Review Date: September 2023

Version: 2.0

Approving Body: Resources Committee

Contents

	Policy Updates	3
	Statement of Intent	4
1	Introduction	4
2	Definition	4
3	Legal Framework	4
4	Roles and Responsibilities	5
5	Objectives	6
6	Purpose and Justification	6
7	Operation of the System/Security	6
8	Data Protection	7
9	Monitoring Procedures	8
10	Media Procedures	8
11	Breaches of the Code (including Breaches of Security)	9
12	Assessment of the Scheme and Code of Practice	9
13	Complaints	9
14	Code of Practice	9
15	Access	10
16	Monitoring and Review	10

Policy Updates

Date	Page	Policy updates
24.06.22	4	Legal framework - addition
24.06.22	6	Operations of the System/Security - addition
24.06.22	7	Data Protection – ‘Privacy by Design’ from previous copy removed and renamed with updated information
24.06.22	9	Code of Practice - addition
24.06.22	10	Monitoring and Review - addition

Statement of Intent

Hope Sentamu Learning Trust takes responsibility towards the safety of staff, visitors and pupils very seriously. To that end, the Trust uses surveillance cameras to monitor any instances of aggression or physical damage to the academies/schools within the Trust.

The purpose of this policy is to regulate the management, operation and use of the surveillance and closed-circuit television (CCTV) system in the academies/schools within Hope Sentamu Learning Trust where applicable, hereafter referred to as 'the academy/school'.

The CCTV Scheme will be registered with the Information Commissioner under the terms of the UK General Data Protection Regulation and will seek to comply with the requirements of both GDPR and the Commissioner's Code of Practice.

The Trust will treat the systems and all information, documents and recordings obtained and used as data which is protected by GDPR.

Each academy/school will not focus static cameras on private homes, gardens and other areas of private property.

Unless an immediate response to events is required, each academy/school will not direct cameras at an individual, their property or a specific group of individuals, without authorisation being obtained using the academy's/school's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Media forms will only be released for use in the investigation of a specific crime and with the written authority of the Police. CCTV footage will never be released to the media for purposes of entertainment.

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.

Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the academy/school CCTV.

The CCTV system will be registered with the ICO in line with data protection legislation.

Signed by:

_____ Headteacher/Principal Date: _____

_____ Chair of Governors Date: _____

1. Introduction

- 1.1. The system comprises of:
 - Cameras - fixed
 - Cameras - dome
- 1.2. The Code of Practice will be subject to review periodically, but at least biennially, to include consultation as appropriate with interested parties.
- 1.3. The CCTV system is owned by the academy/school.

2. Definition

- 2.1. The CCTV is the 'Closed Circuit Television System' which is used within the academy buildings and grounds only. The system is monitored locally within each academy and is used for 'Application' purposes only.
- 2.2. Surveillance- monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. Real-time recordings and live streams. For the purpose of this policy only video and audio footage will be applicable.
- 2.3. Biometric data – data which is related to the physiological characteristics of a person, which confirm the unique identification of that person such as fingerprint recognition, facial recognition (FRT), or iris recognition.

3. Legal Framework

- 3.1. This policy has due regard to legislation, including but not limited to the following:
 - General Data Protection Regulation (GDPR) 2018
 - UK General Data Protection Regulation
 - Data Protection Act 2018
 - Freedom of Information Act 2000
 - Protection of Freedoms Act 2012
 - School Standards and Framework Act 1998
 - Children Act 1989 and 2004
 - Equality Act 2010
 - Surveillance Camera Code of Practice 2013
 - Regulation of Investigatory Power Act 2000
 - The Education (Pupil Information)(England) Regulations 2005 (as amended in 2016)
- 3.2. This policy has been created with regard to the following statutory and non-statutory guidance:
 - 'The Surveillance Camera Code of Practice' - Home Office (2013)
 - 'Guide to the UK General Data Protection Regulation (UK GDPR) ICO 2021
 - 'In the picture: A data protection code of practice for surveillance cameras and personal information' ICO (2017)
 - ICO (2022) 'Video Surveillance'

4. Roles and Responsibilities

4.1. Trust Board

The Trust Board is ultimately responsible for the systems and ensuring compliance with each academy.

4.2. Data Protection Officer (DPO)

The role of the Data Protection Officer (DPO) includes:

- Dealing with Freedom of Information requests and Subject Access Requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the academy handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the academy, their rights for the data to be destroyed and the measures implemented by the academy to protect individuals' personal information.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the academy's Data Protection Impact Assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the academy to relevant personnel.

4.3. Principal

The Principal is responsible for:

- Delegating day-to-day matters relating to data protection to designed personnel.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the academy is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

4.4. Designated Person/s

The designated person/s deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy, will act as the data controller.

4.5. Data Controller

The role of the Data Controller includes:

- Processing surveillance and CCTV footage legally and fairly.

- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure - especially when processing over networks.

5. Objectives

- 5.1. To protect the academy building and their assets. The systems function is to:
- Maintain a safe environment
 - Ensure the welfare of pupils, staff and visitors
 - Deter criminal acts against persons and property
 - Assist the Police in identifying persons who have committed an offence

6. Purpose and Justification

- 6.1. The academy will only use surveillance cameras for the safety and security of the academy and its staff, pupils and visitors.
- 6.2. Surveillance will be used as a deterrent for violent behaviour and damage to the academy.
- 6.3. The academy will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in classrooms or any changing facility.
- 6.4. If the surveillance and CCTV systems fulfil their purpose and are no longer required the academy will deactivate them.

7. Operation of the System/Security

- 7.1. The system will be administered and managed by the **Principal**, in accordance with the principles and objectives expressed in the code.
- 7.2. The CCTV system will be operated 24 hours each day, every day of the year.
- 7.3. The Site Team will check and confirm the efficiency of the system on a monthly basis and that the equipment is properly recording and that cameras are functional.
- 7.4. In exceptional cases where large amounts of information need to be collected and retained, the school will consider using cloud storage. This will be secure and only accessible to authorised individuals.
- 7.5. The ability to produce copies of information will be limited to the appropriate staff.
- 7.6. Access to the CCTV monitors and the recordings will be strictly limited to the Senior Leadership Team (including the Principal's PA), the Site Team and any member of staff who has been delegated authority by the Principal.
- 7.7. Surveillance and CCTV systems will not be intrusive.
- 7.8. Any unnecessary footage captured will be securely deleted from the system.
- 7.9. Any cameras that present faults will be repaired as soon as possible as to avoid any risk of a data breach.

- 7.10. The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption.
- 7.11. Visual display /control monitors are located in the Reception office.
- 7.12. Staff will be trained in the use of the CCTV system and sanctions will be put in place for those who misuse the security system information.

8. Data Protection

Data collected from surveillance and CCTV will be:

- 8.1. Processed lawfully, as determined by DPIA, or from advice from the DPO.
- 8.2. Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- 8.3. Processed in a transparent manner, meaning that people are informed when their data is being captured.
- 8.4. Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
 - Further processing for archiving data in the public interest
 - Scientific or historical research
 - Statistical purposes
- 8.5. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 8.6. Accurate, and where necessary, kept up-to-date, every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
- 8.7. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- 8.8. The use of surveillance cameras, CCTV and biometric systems, will be critically analysed using a DPIA, in consultation with the DPO.
- 8.9. A DPIA will be carried out prior to the installation of any surveillance, CCTV or biometric system. A DPIA will:
 - Describe the nature, scope, context, and purposes of the processing
 - Assess necessity, proportionality and compliance measures
 - Identify and assess risks to individuals
 - Identify any additional measures to mitigate those risks

If the DPIA reveals any potential security or other data protection issues, the Trust will ensure they have provisions in place to overcome these issues.

Where the Trust identifies a high risk to an individual's interests, and it cannot be overcome, the Trust will consult with the ICO before they use CCTV and the Trust will act on the ICO's advice.

9. Monitoring Procedures

- 9.1. Camera surveillance may be maintained at all times. Approved personnel may have remote access to the CCTV system via their academy hardware for security purposes.

10. Media Procedures

- 10.1. In order to maintain and preserve the integrity of the media used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:
 - a. Before using, each media form must be cleaned of any previous recording.
 - b. The controller shall register the date and time of media form insert, including media reference.
 - c. If copies of the media form are required for the Police, these must be referenced and marked 'copy'.
- 10.2. Media forms may be viewed by the Police for the prevention and detection of crime. A register will be maintained of the release of media form to the Police or other authorised applicants. The register will be available for this purpose.
- 10.3. Viewing of Media by the Police must be recorded in writing and in the register. Requests by the Police can only be actioned under Section 19 of GDPR 2018.
- 10.4. Should a media form be required as evidence, a copy may be released to the Police under the procedures of the Code of Practice for Surveillance cameras and personal Information 2017. Media will only be released to the Police on the clear understanding that the media form remains the property of the academy and both the media form and information contained on it are to be treated in accordance with this Code. The academy/school also retains the right to refuse permission for the Police to pass to any other person the media form or any part of the information contained thereon.
- 10.5. The Police may require the academy to retain the stored media for possible use as evidence in the future. Such media will be correctly indexed and securely stored until they are needed by the Police.
- 10.6. Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Principal.

11. Breaches of the Code (including Breaches of Security)

- 11.1. Any breach of the Code of Practice by academy staff will be initially investigated by the Academy's Vice Principal, Ms Holly Lockyer, in order for them to take the appropriate disciplinary action. Any breach of the Code will be reported to the Board of Trustees.
- 11.2. Any serious breach of the Code of Practice will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

12. Assessment of the scheme and code of practice

- 12.1. Performance monitoring, including random operating checks, may be carried out by the Vice Principal, Ms Holly Lockyer.

13. Complaints

- 13.1.** Complaints about the academy's CCTV system should be addressed to the **Principal**.
Complaints will be investigated in accordance with this Code and the Trust's Complaints Procedure.

14. Code of Practice

- 14.1.** The academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- 14.2.** The academy notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails
- 14.3.** CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- 14.4.** All surveillance footage will be kept for a period of four weeks for security purposes; the Principal is responsible for keeping the records secure and allowing access.
- 14.5.** The academy has a surveillance system for the purpose of the prevention and detection of crime and the promotion of health, safety and welfare of staff, pupils and visitors.
- 14.6.** The surveillance and CCTV system is owned by the academy and images from the system are strictly controlled and monitored by authorised personnel only.
- 14.7.** The academy will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the academy, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the academy website.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point which enables people to request information and submit complaints via the DPO.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Only be used for the purpose for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

15. Access

- 15.1.** The General Data Protection Regulations (GDPR) provides Data Subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV. See the Trust's Subject Access Request Policy and Procedures for further details.
- 15.2.** All media containing images belong to, and remain the property of the academy.
- 15.3.** The academy will verify the identity of the person making the request before any information is supplied.

15.4. Requests by persons outside the academy for viewing or copying disks, or obtaining digital recordings, will be assessed by the Principal, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

16. Monitoring and Review

This policy will be monitored and reviewed on **an annual basis** by the Trust. The Principal will communicate changes to this policy to all members of staff.