

Southport Education Group

CCTV Policy

Policy written by: Paris Bonwick	Job title	Vice Principle of Business Services	
	Department	Senior Leadership Team	
Date policy updated	01/02/2024	Date policy to be reviewed	01/02/2025
Impact assessed by	PB	Date impact assessed	01/02/2024

Contents

1.0 Purpose and Scope.....	2
2.0 Operating Principles.....	2
3.0 Rights in relation to Automated Decision Taking.....	2
4.0 Operational Management	2
5.0 Purpose of CCTV System Installation	2
6.0 Data/Privacy Protection.....	3
7.0 Overview of CCTV System.....	3
8.0 CCTV Control of Viewing and Access to Data.	3
9.0 Data Protection	4
10.0 Signage	4
Annex A Southport Education Group CCTV Contractors Agreement	5
Annex B Third Party CCTV Access Request form.....	6
Annex C CCTV Release – Quick Reference Guide And Checklist.....	8

Southport Education Group College: CCTV Policy

1.0 Purpose and Scope

It is the policy of the College to provide a safe work environment for employees, students, visitors, temporary staff and contractors while on the College premises and within the College buildings. CCTV cameras are deployed at various locations within and around the College estates, to assist in the prevention and detection of crime, and to increase the safety of staff, students and visitors on College premises.

This policy details the operating standards and procedures for closed circuit television (CCTV) systems installed at the Southport Education Group, in accordance with the requirements of:

- UK General Data Protection Regulation (GDPR)
- The CCTV Code of Practice 15/10/2014 issued by the Information Commissioners Office.
- Article 8 of the Human Rights Act Right 1998. Respect for Private and Family Life.

2.0 Operating Principles

To ensure compliance with the above, all CCTV operations, must at all times, adhere to the following principles.

- Fairly and lawfully processed.
- Adequate, relevant and not excessive.
- Accurate.
- Images are not retained for longer than is justifiably necessary.
- Processed in accordance with the individual's rights.
- Secure.

3.0 Rights in relation to Automated Decision Taking

Article 22 of the GDPR. Southport Education Group CCTV system is not used in any manner in relation to automated decision taking.

4.0 Operational Management

The CCTV operation management is the responsibility of the Vice Principle of Business Services or the Head of Facilities

5.0 Purpose of CCTV System Installation

The system's overall aims are to help to secure a safer environment for those who study or work at the College by:

- Assisting in the reduction of crime, anti-social behaviour, the fear of crime and increase the confidence of the public in the area.
- Facilitate the identification of offenders.
- Assisting in the prevention and detection of crime and disorder committed in public areas.
- Dealing with any serious public safety concerns.
- Monitoring the security of the College's business premises.
- Ensuring that health and safety rules and College procedures are being complied with.
- Assisting with the identification of unauthorised actions or unsafe working practices that might result in disciplinary proceedings being instituted against employees and to assist in providing relevant evidence.

The system will only be used for these objectives, and for no other purposes.

6.0 Data/Privacy Protection

The College named Data Protection Officer is Clerk to the Corporation and Data Protection Officer, Lisa Farnhill. The Vice Principle of Business Services or the Head of Facilities is the authority with regard to requests under the terms of the Freedom of Information Act and requests from Data Subjects (persons whose images have been recorded by the system).

7.0 Overview of CCTV System

CCTV cameras are installed at various strategic points around the site.

The system comprises of: fixed position cameras, pan, tilt and zoom (PTZ) cameras; monitors; multiplexers, operating software, digital recorders and public information signs.

8.0 CCTV Control of Viewing and Access to Data.

All viewing and observing of the CCTV images will be carried out at Southport Education Group on the appropriate campus. All requests to view footage, whether granted or denied, must be logged. No unauthorised access to the CCTV screens will be permitted at any time. Access will be strictly limited to the security officers, the Data Protection Officer, Safeguarding Team, Vice Principle of Business Services or the Head of Facilities.

CCTV viewing or observing in other places will only take place if authorised by a Data Controller listed above. This includes remote viewing.

All staff working in the viewing area will be made aware of the sensitivity of handling CCTV images and recordings.

The Vice Principle of Business Services or the Head of Facilities will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

Contractors working on the system will sign an undertaking that they understand and will comply with Southport Education Group, CCTV Policy through the contractor management procedure (See Annex A). Images are retained on a secure hard drive for up to 30 days but more likely to be 14 days; after this period, they are automatically over written. Subject to the appropriate data subject access request being made, images are either shown to the requestor, or shared via encrypted transfer, or encrypted disc. Staff must always complete the checklist (Annex C) ahead of providing access to or copies of images.

The downloads are recorded in the CCTV folder which is located in the CCTV Room Office and is signed by the receiving authority/person. In order to carry out this process, images are initially copied to a secure drive within the college system. Should there be any further requests, or if there has been a technical issue, these images are retained on the CCTV Room drive for up to 12 months for reasons of ensuring footage is available for any resulting court action.

The

The College's CCTV system is recording images 24 hours a day seven days a week, 52 weeks a year.

Footage is not retained for longer than is necessary and is automatically erased after 14 days, unless a request to retain footage has been made. On occasion, it could be necessary to retain images for a longer time-period (e.g. during an investigation).

The CCTV system is provided and operated in a manner that is consistent with an individual's right to privacy. However, the system will capture and retain images of persons, even though they are not the main subject of surveillance.

Only a limited number of authorised staff may access the system and all access must be logged, including any requests to view which are denied.

Live monitoring – Security (restricted viewing access).
Live monitoring and playback – authorised Estates staff.
Live monitoring and playback – authorised Safeguarding staff.

9.0 Data Protection

The CCTV system is registered with the Information Commissioners Office (ICO) under the terms of the DPA2018 and the UKGDPR.

Under the definitions within the Data Protection Act (DPA) 2018, CCTV pictures viewed and/or recorded constitute data.

Where individuals may be identified from the material, images will be considered personal data under the Act and will therefore be subject to the College's policy on Data Protection.

In line with the College's policy on Data Protection, and Subject Access requests, data subjects are entitled to access personal data, including CCTV images. All requests are subject to exclusions, limitations and exemptions as outlined within that policy. Images will not be provided to a third party except for law enforcement bodies or to comply with the DPA2018.

Requests for access to view /copy CCTV footage should be made to:

dataprotection@southport.ac.uk

The request should clearly detail:

- The reason for the request.
- The date and time that the images were recorded
- Any information that can help some one identify themselves
- The location of the CCTV camera
- Proof of identity

The College will then respond to the request within 30 days.

10.0 Signage

CCTV signs are placed at various points around the College premises to inform staff, students, visitors and the general public that CCTV is in operation, the purpose of the CCTV and details of the operator.

Southport Education Group CCTV Contractors Agreement



By undertaking work on the system, I confirm that I have read and understand the Colleges CCTV Policies and Data Protection Policy. And confirm to adhere to these. No data will be exported off the system during this work that we are undertaking.

Company Name

Full Company Name

Contractor undertaking work Full name.

Address (including full postcode)

Telephone no.

Work email

Signed: _____

Print: _____

Date: _____



Southport Education Group CCTV Access Request form: Police and third parties

How third parties can access information from us.

This form is to be used by police, solicitors or court representatives requesting CCTV footage for investigations or court proceedings.

Contact details

Full name of police officer or third party *

Police officer badge number

Police station:

Address of third party (including full postcode) *

Crime Incident ref no, or Court case ref no *

Telephone no. *

Work email*

Give details of the incident under investigation or subject to court proceedings *

Information to enable us to deal with this request

Location of the CCTV camera (e.g. the canteen, reception or car park) *

If you're seeking access to a particular image (if known) please indicate below

Date and time the image would have been recorded (please estimate):

Please provide description of the person or incident you are investigating:

If known, please provide the name of the Southport Education Group employee you have been dealing with about this incident or investigation:

Declaration

Please tick the box to declare that the information given in this form is true *

I confirm that I am making this request under one of the following exemptions in DPA 2018 Schedule 2 (please tick which one applies)

- For crime and taxation purposes, OR
- By order of the court or for legal advice/ proceedings

Signed: _____ Print: _____

Date: _____

Southport Staff use only:

ID checked (tick to confirm):

Date images provided: _____

Signed (staff): _____ Print name: _____



Annex C

CCTV Release – Quick Reference Guide And Checklist

For more information go to:

<https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/>

There are limited circumstances in which CCTV footage can be accessed or shared.

Please refer to our CCTV policy for more information on what we record, why and who it is shared with.

Unless you are familiar with the requirements, contact the DPO before you access or release **ANY** images.

Remember, even when the request is in relation to law enforcement, we are still obliged to comply with GDPR and think about what we are giving, why and to who. Data minimisation is still relevant, only give what is necessary and carefully record your actions.

Checklist

- Consider what the purpose is for sharing personal data with law enforcement authorities, and whether it is necessary and proportionate to do so.
- Identify a lawful basis under Article 6 of the UK GDPR before sharing the personal data. If the sharing of personal data was not the original intention of the processing, consider whether this new purpose is compatible with that original purpose. There is an [interactive tool](#) to help you. (article 6 c – lawful basis is usually used for criminal investigations)
- Also identify a condition for processing under Article 9 of the UK GDPR and any relevant condition in Schedule 1 of the DPA 2018 before sharing special category data.
- We identify a condition for processing under Article 10 of the UK GDPR and a relevant condition in Schedule 1 of the DPA 2018 before sharing criminal offence data.
- Record our lawful basis and, if relevant, our conditions for processing special category or criminal offence data. (Use the CCTV access log to record this)
- Only the minimum necessary amount of relevant and adequate personal data has been included.
- Ensure that the personal data is shared in compliance with our other data protection duties and obligations, including fairness, accuracy and security.

