

# CCTV Policy

|                     |                             |
|---------------------|-----------------------------|
| Policy Originator:  | Susanne Wicks, DPO          |
| Approved by:        | CLT                         |
| Date Approved:      | Spring 2026                 |
| Review Interval:    | Three years or as required. |
| Next Review Date:   | Spring 2029                 |
| Audience:           | Internal                    |
| Entered on SP:      | October 2026                |
| Entered on website: | October 2026                |

## Introduction

As part of its commitment to ensuring a safe and secure environment for students, staff and visitors, Nescot has a closed circuit television (“CCTV”) system in place. CCTV systems are based around digital technology and therefore must be treated as information that will be processed under the Data Protection Act 2018. The person ultimately responsible for data protection in Nescot is the CEO/Principal, but any enquiries should be directed to [data.protection@nescot.ac.uk](mailto:data.protection@nescot.ac.uk)

The purpose of this Policy is to regulate the management, operation and use of the CCTV system at the colleges. This document sets out the accepted use and management of the CCTV system and images to ensure that Nescot complies with relevant guidance and legislation, including:

- [UK General Data Protection Regulation](#)
- [Data Protection Act 2018](#)
- [Human Rights Act 1998](#)
- [European Convention on Human Rights](#)
- [The Regulation of Investigatory Powers Act 2000](#)
- [The Protection of Freedoms Act 2012](#)
- [The Freedom of Information Act 2000](#)
- [The Education \(Pupil Information\) \(England\) Regulations 2005 \(as amended in 2016\)](#)
- [The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations 2004](#)
- [The Equality Act 2010](#)
- [Surveillance Camera Code of Practice](#)
- [Guidance from the Information Commissioner.](#)

## Purpose of CCTV

Nescot has installed CCTV to:

- Protect the buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption
- To increase the personal safety of staff and students and reduce the fear of physical abuse, intimidation and crime.
- To assist in the prevention and detection of crime.
- Assist with the identification, apprehension and prosecution of offenders.
- Assist with the identification of actions/activities that might result in disciplinary proceedings against staff and students.
- Assist in the usage and management of the College buildings on a day to day basis.
- Provide management information relating to contract compliance of third party service providers.

- Monitor security of campus buildings.
- Identify vehicle movement around the campus.

The system will be provided and operated in a way that is consistent with an individual's right to privacy.

## **Operation**

The CCTV surveillance system is owned by Nescot. The Head of Estates and Facilities is responsible for the day-to-day operation of the system and ensuring compliance with this policy. The Security Manager holds an SIA CCTV Licence.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements both of the Data Protection Act 2018 and the Commissioner's Code of Practice.

Cameras will be used to monitor activities within the College buildings, car parks and other areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the occupants within the College grounds, together with its visitors.

Static cameras will not focus on private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV system will not be used for any commercial purpose. Downloads will only be released to the media for use in the investigation of a specific crime and with the written authority of the police.

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

Information notices, as required by the Code of Practice of the Information Commissioner, have been placed at access routes and areas covered by the college CCTV System.

## **Image Viewing and Download Procedure**

Footage of students and visitors may be viewed only by the following Authorised Officers:

- Members of the Executive Leadership Team
- The Vice-Principal.
- The Assistant Principal (Learning Support and Student Experience).
- Permanent members of the Security Team.

Other staff may request to view footage via completion of [this form](#). Once approved by the Data Protection Officer, the request will be passed to the Security Team who will arrange for the footage to be shared.

Recordings of staff may only be viewed with advance permission from the Chief People Officer. Requests to view footage of staff must be made via [this form](#).

Police may make a request for CCTV footage, but all requests from the Police and any other external agency must be directed to the Data Protection Officer in the first instance. This may include prosecution agencies, insurance companies or legal representatives.

Images will never be released to the media for purposes of entertainment.

## **Breaches of this Policy**

Misuse of the system may be a criminal offence. Any suspected breach of this Policy by Nescot staff will be considered under Nescot's Disciplinary Policy and Procedures.

## **Overview of System**

The CCTV system operates 24 hours a day, seven days a week, and records continuously.

The system comprises fixed-position cameras, pan-tilt-zoom (PTZ) cameras, monitors, digital recorders, and public information signs.

CCTV cameras are located at strategic points on site, principally at the entrance and exit point for the site and various buildings, as well as main thoroughfares throughout the site. We have also installed cameras in toilets where repeated instances of vandalism, drug use, or other serious misconduct have occurred. These areas have been carefully selected based on a clear pattern of damage, antisocial behavior, and security risks. The goal of this surveillance is to deter such activities, protect public property, and ensure a safe and clean environment for all users. Additionally, if issues persist, the footage can help identify those responsible, allowing for appropriate action to be taken.

CCTV signs are prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV installation is in use, its purpose and details of the operator.

Although every effort has been made to ensure maximum effectiveness of the CCTV system; it does not cover all areas and it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

## **Data Protection Act 1998**

For the purpose of the Data Protection Act 2018, Nescot is the data controller.

CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act 2018. This policy is associated with the College's Data Protection Policy, the provisions of which should be adhered to at all times.

The College has registered its processing of personal data (including CCTV) with the Information Commissioner's Office (ICO).

Where new cameras are to be installed on College premises, the ICO's CCTV Code of Practice will be followed before installation:

- The appropriateness of and reasons for using CCTV will be assessed and documented;
- The purpose of the proposed CCTV system will be established and documented;
- Responsibility for day-to-day compliance with this policy will be established and documented;

Additional CCTV cameras shall be installed at the recommendation of the Head of Estates and Facilities, following completion of a data protection impact assessment and consultation with the Chief Operating Officer and Data Protection Officer. Any requests to install CCTV shall be carefully considered on the basis of risks to the college community and will take into account evidence of vandalism, anti-social behaviour or security risks. The impact assessment is available [here](#).

## **Individual Access Rights**

The Data Protection Act 2018 gives individuals the right to access personal information about themselves, including CCTV images. All requests for access to view/copy CCTV footage by individuals will be dealt with as a subject access request. All applicants should be directed to the Data Protection Officer for advice.

## **Retention and Disposal**

Recorded images will be retained for no longer than 31 days from the date of recording, unless required for evidential purposes or the investigation of crime or otherwise required and retained as a download with the requisite approval form.

All images on electronic storage will be erased by automated system overwriting. All downloads, still photographs and hard copy prints will be securely disposed of as confidential waste.

## **Responsibilities**

- The Data Protection Officer is responsible for producing and reviewing this Policy.
- The College Leadership Team is responsible for approving this Policy.
- The Head of Estates and Facilities is responsible for compliance with and implementation of procedures to comply with this policy.

## **Complaints**

Complaints regarding the CCTV system and its operation should be made via Nescot's complaints procedure.

## **Covert Recording**

Prior to authorisation, the requesting applicant must have demonstrated and documented that all reasonable procedures and practices were put in place to prevent suspected illegal or unauthorised activity from taking place. Requests should be made via [this e-form](#).

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom. Legal advice may be sought when approving and assessing the need for covert recording in all instances.

Covert cameras may be used under the following circumstances, with the authorisation of the Data Protection Officer and CEO/Principal:

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording.
- That there is reasonable cause to suspect that illegal activity is taking place or is about to take place or unauthorised activity is taking place; that may seriously or substantially affect the operation or reputation of the College.
- A record of data destruction will be made in confirmation on the authorised request to make covert recordings.