# CCTV Policy

| | |
|---|---|
| Author | Director of IT |
| Date | December 2024 |
| Person Responsible | Director of IT |
| Approval/review body | SLT |
| Frequency of Review* | 36 months |

** Policies will be reviewed more frequently if legal changes or good practice require*

| **Review History:** | | |
|---|---|---|
| **Date** | **Reviewed by** | **Reason for review** |
| Mar 2023 | Director of IT &<br>Head of Estates / Risk Management | Created in response to internal audit requirement. |
| Dec 2024 | Director of IT &<br>Head of Estates / Risk Management & DPO | Review |

## Contents


1. Statement ..... 2
2. About this Policy ..... 2
3. Key principles ..... 2
   - 3.1 Integrity ..... 2
   - 3.2 Confidentiality / Data Protection ..... 3
   - 3.3 Legality ..... 3
4. Purpose of CCTV ..... 3
5. Covert Recording ..... 3
6. CCTV Owner and Management ..... 4
7. CCTV Operation and Access Procedures ..... 4
8. CCTV Regulation ..... 6

Appendix A – Applicable Legislation ..... 7

- Data Protection Act 2018 and UK General Data Protection Regulation ..... 7
- Regulations of Investigatory Powers Act 2000 (RIPA) ..... 8
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699) ..... 8
- Human Rights Act 1998 (HRA) ..... 9

Appendix B – CCTV Authorised Managers and Operators ..... 11

Appendix C - Guidelines for authorised CCTV Managers / Operators ..... 12


**Related Policies and Procedures:**

Data Breach Policy and Procedure
Data Protection Policy and Procedure
IT Conditions of Use Policy
Staff Code of Conduct
Staff Disciplinary Policy and Procedure

**NOTE**: This Policy together with the Policies and Procedures listed above, seeks to ensure, so far as reasonably practicable, that the College is fulfilling its duty under sections 26 and 29 of the Counter-Terrorism and Security Act 2015 and the Prevent Duty. The College will participate fully to prevent people from being radicalised or drawn into extremism and will ensure that, should this occur, there are procedures in place to deal with them.

## 1. Statement

To create safe working and learning environments for all students, staff and visitors, North Kent College ("the **College**") which incorporates Hadlow College, operates multiple closed circuit television surveillance systems ("CCTV") to record images and video ("CCTV Data"). In a limited number of areas, such as Receptions, the CCTV Data will include audio.

The CCTV systems utilise Information Technology ("IT") networking and digital hardware and software facilities.

## 2. About this Policy

2.1 Sets out the College's policy for staff in matters relating to the monitoring of college premises and facilities using CCTV.

2.2 The College operates multiple independent CCTV systems that are used as set out in Section 4 below.

2.3 The CCTV systems may capture images, video or audio of an individual and so all CCTV Data is considered to be Personal Data and as such, will be processed in compliance with current UK Data Protection Laws.

2.4 The College will also have due regard to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998.

Although not a Relevant Authority, the College will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and the 12 guiding principles contained therein. The College has produced this policy in line with the Information Commissioner's Office ("ICO"), CCTV Code of Practice.

## 3. Key principles

The following Lawful Bases applies to the College's use of CCTV:

- Legitimate Interest
- Protecting the vital interests of individuals

Staff are required to observe the following precepts in relation to CCTV:

### 3.1 Integrity

The accuracy and completeness of information captured by the CCTV within the College must be safeguarded.

3.2 **Confidentiality / Data Protection**

The security of CCTV Data must be protected from unauthorised access, disclosure, or interception.

3.3 **Legality**

Material held or transmitted using the College's IT and communications system must respect copyright and conform to national and international law.

## 4. Purpose of CCTV

The College uses CCTV for the following purposes;

4.1 to increase the personal safety of students, staff and visitors and reduce the concern of physical abuse, intimidation, and crime;

4.2 to protect college property, facilities and equipment and help ensure they are kept free from intrusion, vandalism, damage, or disruption;

4.3 to assist in deterring theft (loss prevention) and to deter inappropriate behaviour;

4.4 assist in the detection and reporting of crime;

4.5 provide evidence of crime;

4.6 provide management information with regard to health and safety;

4.7 to support investigations into reported accidents/ incidents.

4.8 provide management information to assist in the operation of college policies;

4.9 to support insurance claims for damage to college property, equipment;

4.10 to support the police or other law enforcement authorities in their investigations and pursuit of prosecutions;

4.11 to identify and manage vehicle movement around all college campuses; and

4.12 assist the Police and civil authorities in the event of a major emergency.

Other than where necessary and permitted in Law, the CCTV systems will NOT be used in any fashion to breach any individual's privacy.

## 5. Covert Recording

The College does not, as a matter of course, carry out covert CCTV recording and will only do so by exception and where permitted in Law to do so.

Except as stated above, the CCTV systems used by the College are fixed or moving cameras that are always visible. Appropriate signage is posted in strategic areas (for example entrances and exits) where CCTV is in operation.

CCTV cameras are usually motion activated and will record until the activity stops.

Unless required for evidential purposes or the investigation of crime or otherwise required by law, CCTV data will be retained for up to 31 days from the date of recording.

## 6. CCTV Owner and Management

The CCTV systems are owned by the College and appropriate signage is displayed at strategic points. Campus entrances and exits for example.

Most College CCTV systems are managed and operated by the College Estates and Risk Management Team staff, however, there are some systems installed into specific areas that are operated and managed by the Departments responsible for those areas.

All CCTV systems MUST be registered with the IT Department and any new systems MUST be authorised by the Director of IT. Authorised operators and manager must be included and updated annually, or sooner, if changes occur in the interim.

The most recent guidelines for operation (supplied by the Data Protection Officer ("DPO")) MUST be posted at CCTV control consoles for operators to be aware of the policy regarding the use of CCTV.

Responsibility for the installation and maintenance of CCTV systems is with the IT Department (Director of IT).

Responsibility for security of the data captured by the CCTV systems rests with the responsible manager (see Appendix B)

Monitoring the College's compliance with the Data Protection Laws rests with the DP

## 7. CCTV Operation and Access Procedures

The College CCTV systems include static and Pan Tilt Zoom ("PTZ") moving cameras. In certain circumstances (for example Residential Support Officers) body worn cameras may also be utilised.

Static cameras will not capture images of private homes, gardens, or other areas of private property.

Operators of PTZ cameras, will only use this capability to follow individuals that are behaving suspiciously or are in the commission of a crime.

Body worn CCTV cameras will ONLY be turned on and used once the individual being recorded has been notified.

CCTV data will NOT be used for any commercial purpose nor uploaded to the Internet for any commercial purpose.

Access to CCTV Data will be restricted to those staff that have been authorised as set out at Appendix B.

Disclosure of CCTV Data will only be made in strict accordance with the Purposes of the system (see Section 4) and as set out in this section.

The procedure for reviewing and/ or downloading of CCTV footage is as follows:

7.1. All retrospective requests for CCTV data of incidents in the College MUST be logged via the Estates HelpDesk system. This log MUST include date, time and location and should also include a description of the incident for the CCTV operator. Only authorised CCTV managers / operators may view or download (for evidence) CCTV footage. Appendix B shows a list of CCTV systems and authorised mangers / operators.

7.2. Any CCTV Data related to the logged incident must be stored securely by the CCTV manager / operator and may NOT be viewed or copied by non-authorised staff (staff not listed as authorised in appendix B), or any other person without the express permission of the College DPO, Head of Estates & Risk Management, or their Deputies.

7.3. Any downloads of CCTV data relating to logged incidents MUST only be retained for as long as is necessary for the Purpose and in a secure Microsoft OneDrive or Teams site location. Once no longer required, the CCTV Data must be deleted.

7.4. Where the need to view live or recorded CCTV data is urgent, a Manager or a more senior member of staff must be notified, unless there is imminent threat to life. A request for the incident must be logged retrospectively on the Estates Helpdesk as described in 7.1 above.

7.5. Freedom of Information requests for CCTV data must be made in writing to the NKC Director of People and any release of such data MUST be authorised by the Deputy Chief Executive Officer before release.

7.6. Police and other law enforcement agencies requesting access to, or copies of, CCTV data must provide a properly completed and signed “Disclosure of Personal Information” request (as per Data Protection Act 2018 s35(2)).

7.7. Downloads requested for any purposes Purpose outside those set out at Section 4 of this policy are NOT permitted.

7.8. In all cases, CCTV data will ONLY be provided to the authorised persons/authorities as described above once approved by the College DPO, Head of Estates & Risk Management or their deputies and may ONLY be shared using Microsoft OneDrive or another equally secure method.

The guidelines for authorised CCTV managers / operators are shown in appendix C.

## 8. CCTV Regulation

For the UK Data Protection Act 2018 the Data Controller is:

North Kent College

The NKC Data Protection Officer can be contacted on dpo@nothkent.ac.uk

The College is required to register its processing of personal data (including CCTV) with the ICO. The College's ICO registration number is **Z6685902,** which is renewed annually.

## Appendix A – Applicable Legislation

- Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) (together known referred to as the UK Data Protection Legislation) and guidance in the Information Commissioner's Employment Practices Data Protection Code.

Monitoring employee use of email and the internet involves the processing of personal data.

The six data protection principles under UK Data Protection Legislation and Part 3 of the Employment Practices Code (monitoring at work) are relevant when monitoring is carried out, but some are more significant than others:

1. processed fairly and lawfully (*first data protection principle*);
2. collected only for specified lawful purposes and shall not be processed in a manner incompatible with those purposes (*second data protection principle*);
3. adequate, relevant and not excessive for the purposes for which they are processed (*third data protection principle*);
4. accurate and, where necessary, kept up to date (*fourth data protection principle*);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; *(fifth data protection principle*); and
6. 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, using appropriate technical or organisational measures ('integrity and confidentiality'). (*sixth data protection principle*);

In respect of the College's compliance with the Employment Practices Code regarding monitoring at work it has regard to the core principles of the Code and the College:

1. recognises that worker's private lives usually extend into the workplace and employees have an expectation of privacy, even where they have been informed monitoring may take place;
2. ensures that appropriate impact assessments are carried out;
3. that its monitoring is justified and proportionate;
4. the need to inform employees that monitoring is to take place; and
5. ensures that only a limited number of staff have access to information obtained through monitoring.

- Regulations of Investigatory Powers Act 2000 (RIPA)

RIPA 2000 consolidates a range of law enforcement investigative powers in respect of computer and electronic communications. It regulates certain types of monitoring.

Under RIPA 2000 an interception occurs when some or all of the content of a communication is made available during its transmission to a person other than the sender or the intended recipient. This includes any storage of the communication in the telecommunications system before its receipt, such as voicemail that has not been listened to or an unread e-mail.

It is an offence for a person to "intentionally and without lawful authority to intercept…any communication in the course of its transmission by means of either (a) a public telecommunication system or (b) a private telecommunication system.

The lawful interception of communications can however take place if the interceptor has reasonable grounds for believing that both the sender and the recipient have consented to the interception.

- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)

Businesses can monitor or record communications without consent to:

1. ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business;

2. ascertain or demonstrate standards which are or ought to be achieved by persons using the system;

3. prevent or detect crime;

4. investigate or detect the unauthorised use of the telecommunications system;

5. ensure the effective operation of the system.

Businesses are also allowed to monitor, but not record without consent for the purpose of:

1. determining whether the communications are relevant to the business; and/or

2. monitoring communications to a confidential anonymous counselling or support helpline.

- Human Rights Act 1998 (HRA)

Only public authorities are expressly subject to the HRA. The College falls in this category. Article 8(1) of European Convention of Human Rights ("ECHR") states "everyone has the right to respect for his/her private and family life, his/her home and his/her correspondence".

This, however, is not an absolute right and a public authority is permitted to monitor for the prevention of disorder or crime, protection of health or moral and for the protection of the rights and freedoms of others subject to the doctrine of proportionality. The College has regard to its obligations under the HRA and ECHR and is satisfied that the methods chosen for monitoring communications is no more than necessary to accomplish its identified objectives.

- Section 29 Protection of Freedoms Act 2012

(1) The Secretary of State must prepare a code of practice containing guidance about surveillance camera systems.

(2) Such a code must contain guidance about one or more of the following:

(a) the development or use of surveillance camera systems, and/or

(b) the use or processing of images or other information obtained by virtue of such systems.

(3) Such a code may, in particular, include provision about:

(a) considerations as to whether to use surveillance camera systems,

(b) types of systems or apparatus,

(c) technical standards for systems or apparatus,

(d) locations for systems or apparatus,

(e) the publication of information about systems or apparatus,

(f) standards applicable to persons using or maintaining systems or apparatus,

(g) standards applicable to persons using or processing information obtained by virtue of systems,

(h) access to, or disclosure of, information so obtained, and/or

(i) procedures for complaints or consultation.

(4) Such a code:

(a) need not contain provision about every type of surveillance camera system,

(b) may make different provision for different purposes.

(5) In the course of preparing such a code, the Secretary of State must consult:

(a) such persons appearing to the Secretary of State to be representative of the views of persons who are, or are likely to be, subject to the duty under

section 33(1) (duty to have regard to the code) as the Secretary of State considers appropriate,

(b) the Association of Chief Police Officers,

(c) the Information Commissioner,

(d) the Chief Surveillance Commissioner,

(e) the Surveillance Camera Commissioner,

(f) the Welsh Ministers; and

(g) such other persons as the Secretary of State considers appropriate.

(6) In this Chapter "surveillance camera systems" means:

(a) closed circuit television or automatic number plate recognition systems,

(b) any other systems for recording or viewing visual images for surveillance purposes,

(c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or

(d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).

(7) In this section:

- "the Chief Surveillance Commissioner" means the Chief Commissioner appointed under section 91(1) of the Police Act 1997,
- "processing" has the meaning given by section 1(1) of the Data Protection Act

## Appendix B – CCTV Authorised Managers and Operators

| Location | Area | Primary Purpose | Date | Manager | Playback Operators | View Operators | Comments |
|---|---|---|---|---|---|---|---|
| Dartford LTC (Local PVR) | Learning Technologies | Behaviour | 03/07/24 | Head of Learning Technologies | Head of Learning Technologies | | Behaviour management localised system |
| Dartford Miskin Theatre (Local PVR) | Technical Theatre | Behaviour | | Vice Principal | Theatre Business Manager | | Theatre security localised system |
| Dartford Security (NVR in Data Centre with viewing station in Rose Cottage) | Campus | Policy | | Head of Estates and Risk Management | Estates Security Officer | Estates Security Officer | Central system |
| Gravesend Refectory (Local PVR) | Catering | Loss prevention | | Chef Manager | Estates Security Officer | | Localised system |
| Gravesend Motor Vehicle Workshop (Local PVR) | Motor Vehicles | Behaviour and Loss prevention | | Motor Vehicle HOC | Motor Vehicle HOC | | Localised system |
| Gravesend E Block (Local PVR) | Carpentry | Loss prevention | | HOC Construction Crafts | HOC Construction Crafts | | Localised system |
| Gravesend Security (NVR in R block Comms with viewing from security bubble) | Campus | Policy | | Head of Estates and Risk Management | Estates Security Officer | Estates Security Officer Estates Caretaker | Central system |
| Hadlow AMU (Viewing via web) | Animal Management | Animal Monitoring | | AMU HOC | AMU HOC | | Animal welfare local viewing from central system |
| Hadlow Motor Vehicle Workshop (Local PVR) | Motor Vehicles | Loss prevention | | Motor Vehicle HOC | Motor Vehicle HOC | | Localised system |
| Hadlow RRC (Sub NVR connected to central NVR) | Animal Management | Animal Monitoring | | AMU HOC | IT Manager Senior 2nd line IT Technician | AMU HOC | Animal welfare local viewing from central system |
| Hadlow Security (NVR in Data Centre with management from Estates) | Campus | Policy | | Head of Estates and Risk Management | Assistant Estates Manager (W) Estates Officer (W) | | Central system |
| Tonbridge Security (NVR in Data Centre with viewing from IT Department and Health & Safety / Risk via web) | Campus | Policy | | Head of Estates and Risk Management | IT Manager<br>Senior 2nd line IT Technician<br>Risk Manager<br>DPO | | IT Department |

**Appendix C - Guidelines for authorised CCTV Managers / Operators**

To be posted At all CCTV viewing stations

**V3 April 2024**

Use of CCTV by business (including the public sector) is governed by the Data Protection Act (2018) in the United Kingdom.

The North Kent College CCTV policy (available on StaffNet) sets out how the College complies with that Legislation.

**Guidance for authorised CCTV managers / Operators**
(Refer to Section 7 *CCTV Operation and Access Procedures* for full details.)

1. Only authorised staff *(CCTV Policy appendix B)* may view CCTV images/footage.
2. Any request for access to CCTV footage must be logged on the Estates HelpDesk including a description, time, and location of the reported incident.
3. When footage is requested, authorised staff to check if CCTV footage exists for the reported incident.
4. If footage exists, this should be saved in secure OneDrive or Teams location. NOT to be shown to unauthorised staff or 3rd parties.
5. All viewing and downloading of CCTV footage must be recorded on the CCTV Access Log, accessed via the NKC Data Protection StaffNet.
6. Release of CCTV footage can ONLY be authorised by the NKC DPO, Head of Estates & Risk Management, or their deputies and the data must be transferred via OneDrive or another equally secure method.

**NOTE**

1. CCTV footage held on the system will be automatically overwritten based on the settings of that system (maximum retention period is 31 days).
2. Footage downloaded from the system MUST only be stored for as long as necessary for the Purpose for which it was downloaded.

Queries: dpo@northkent.ac.uk