

Closed-Circuit Television (CCTV) – North Yorkshire Police (NYP) estates mounted CCTV Codes of Practice Policy

This document is part of the NYP policy to which all Chief Constable personnel and the functions provided by the Deputy Mayor for Policing as part of the York & North Yorkshire Combined Authority are required to adhere.

1. Policy Statement

This policy statement is open to public viewing from the NYP Website

This Code of Practice explains how NYP will use **estates property mounted** CCTV, taking into consideration national guidance and recommendations outlined in College of Policing Authorised Professional Practice for CCTV in custody and wider legal framework.

2. Aims of the Code of Practice

The aim of the Code of Practice is to ensure North Yorkshire Police;

- 2.1.** Provide clear and unambiguous information on the use of **estates property mounted** CCTV recording equipment.
- 2.2.** Provide a framework of instructions for the use, retention and analysis of **estates property mounted** CCTV recording.
- 2.3.** Meet the requirements of the Data Protection law where personal data is being processed.
- 2.4.** Follow CCTV and Video Surveillance guidance as outlined by the [Information Commissioner's Office](#).
- 2.5.** Meet the twelve principles required by the Surveillance Camera Commissioner under the Home Office Surveillance Camera Code of Practice (as amended 2022):
 - 1.** Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
 3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
 4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
 5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
 6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
 7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
 8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
 9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
 10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
 11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
 12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.
- 2.6. Signpost users to the national standards which North Yorkshire Police adhere to.
 - 2.7. Effectively use estates property mounted CCTV systems to obtain the best value from this asset.
 - 2.8. Meet the requirements of the Health and Safety at Work Act.
 - 2.9. Safeguard the welfare of NYP and NYCA employees and volunteers in their workplace.

- 2.10. Work in line with the Control Strategy aim to reduce community harm.
- 2.11. To develop an expedient, seamless, end-to-end Digital Policing Journey from first contact through to disposal, to better protect and engage the public, reduce the threat of crime, risk and harm, and bring offenders to justice.

3. Responsibilities

- 3.1. The Strategic Lead is the Chief Officer responsible for Estates oversight, or in their absence the nominated deputy.
- 3.2. Infrastructure development and deployment of new cameras is the responsibility of the Head of Estates, Transport and Logistics. It is their responsibility to ensure these will integrate into the system to allow this Code of Practice to operate efficiently and effectively.
- 3.3. All proposals for new infrastructure will be submitted to the Strategic Lead who is responsible for confirming that the proposals are appropriate and proportionate, taking account of strategic assessment and privacy impact assessment, in balancing protection of the public, staff and buildings with the rights and legitimate expectations of individual privacy. The Data Protection Officer (DPO) should be involved in conducting the Data Protection Impact Assessment (DPIA) and considerations around proportionality. That confirmation is required before any development is progressed.
- 3.4. The Strategic Lead will ensure that arrangements are in place for review of the locations of all CCTV at least annually to ensure that the deployment remains appropriate and proportionate and ensure that access rights to the CCTV system are reviewed annually as part of the Information Asset Owner (IAO) responsibilities, in line with the Information Asset Register and the annual Information Asset Review process.

4. Information Governance and Asset Ownership

- 4.1. The CCTV system is classified as an information asset. The designated **Information Asset Owner (IAO)** is responsible for ensuring that:
- The asset is recorded in the Information Asset Register.
 - Access rights are reviewed annually as part of the Information Asset Review process.
 - Risks associated with the asset are identified and mitigated.
 - Compliance with data protection and information security policies is maintained.
- 4.2. The IAO will work in conjunction with the Data Protection Officer and Information Management to ensure that access to the CCTV system remains appropriate, proportionate, and legally compliant.

5. Scope

- 5.1.** North Yorkshire Police currently has an estate of mixed-use facilities including police stations, police custody suites, vulnerable witness investigation suites, and other buildings, some or all of which allow or include access/admission of members of the public as well as North Yorkshire Police Officers and support staff. In addition, other persons may come into contact with the Police's CCTV systems such as employees of companies either directly or indirectly dealing with, or trading with, North Yorkshire Police. As such, people outside of the organisation could potentially be recorded by NYP systems.
- 5.2.** CCTV has become a part of everyday life for the vast majority of the population of Great Britain. The use of CCTV generally within North Yorkshire Police reflects the usage of CCTV systems throughout the country. It is therefore important that NYP are clear about the purposes for which it is recording. This purpose shall fulfil two main criteria:
- to deter criminal and anti-social behaviour at sites where CCTV is operating;
 - to reassure both members of the public and members of staff via the overt use of such CCTV systems thus making the public feel secure.
- 5.3.** North Yorkshire Police, like so many other organisations, employs the use of CCTV on/in many of its buildings both for security purposes and, in the case of custody suites, as a further measure to safeguard both detainees and custody staff.
- 5.4.** As well as providing important safeguards, the use of CCTV also enhances public confidence in the provision of policing, and allows for the recording, storing and retrieval of information over an extended period of time.

6. Purpose

6.1. Police Premises – General Use

CCTV has been installed in Police Buildings for the following purposes:

- To protect the security of the buildings and persons within
- To assist in the prevention and detection of crime and disorder
- To provide real-time information about ongoing incidents
- To assist with the conduct of investigations
- To reduce the fear of crime and help people feel safe
- Increase public confidence
- Promote a safer working environment for staff, detainee's, visitors and any other persons who may come into contact with the CCTV recording system
- Bring more offenders to justice by production of evidence
- Reduce repeat offending
- Reduce complaints
- Valuable tool in ensuring good practice and compliance with Policy and Procedure

CCTV – NYP estates mounted CCTV Codes of Practice Policy

6.2. Police Premises – Custody / Detention

It is now well accepted that CCTV in police custody suites, particularly in police cells and detention rooms, can be a useful tool to assist in the monitoring of vulnerable detainees and thereby help reduce the instances of self-harm. However, the use of cameras in what might normally be regarded as an area where a detainee can expect an element of privacy raises some human rights issues. It is vital therefore that any invasion of the right to privacy is balanced appropriately and sensitively with the need for police officers to effectively discharge their duty of care to persons who are in custody and who are at increased risk of harm. Although covered by additional policy this overarching Code of Practice seeks to cover all NYP owned and managed **Estates property mounted** CCTV where appropriate.

Full guidelines are detailed in [CoP APP Detention and Custody](#) alongside NYP's [CCTV within Custody Procedure](#)

7. Monitoring:

- 7.1. The system can be remotely monitored or monitored at the site dependant on the software / hardware. Where this is an activated camera this is monitored only by retrieval of this data for a legitimate purpose. This monitoring is by specified operational staff dependent upon it being necessary and proportionate to the objective set.

8. Recording, Retention, Removal and Disposal

- 8.1. **Recording** - High definition images and audio captured on camera are recorded 24hrs per day, 365 days of the year or as activated dependant on source.

8.2. Retention:

- All data will be stored for a minimum period of 31 days, then dependant on area it will be routinely overwritten. Any data that is further required for the investigation of incidents or to support criminal prosecutions, will be stored as evidence for as long as there is a policing purpose, as per the APP retention guidelines.
- For detected crimes, under the CPIA code of practice, any relevant CCTV master footage should be retained until the accused is acquitted, convicted or the prosecutor decides not to proceed with the case.
- For detected crimes, where the accused is convicted of the offence, all relevant material must be kept until the convicted person is released from custody, discharged from hospital where the hospital order has been imposed or 6 months from the date of conviction in all other cases.
- For undetected crimes, CCTV evidence should be retained in accordance with MoPI guidance on retention, review and disposal.
- For crimes and incidents relating to custody and custody reception areas, the retention period must be 3 months. However if required for an investigation, they should be held for the length of the investigation and then in accordance with MoPI guidance on retention, review and disposal.

- 8.3. Removal:** Recorded material removed from the system will remain in digital format, emailed or exported where possible. The removal of footage shall be fully auditable. If a disc has to be produced, this is to be fully documented at the point of removal

A production log is held on the system and is automatically generated for EVERY instance in which recorded material is removed from the system electronically.

The audit log documents:

- The date on which the images were removed from the system
- The date and time/period of the footage removed
- The camera(s) the footage was removed from
- The location the footage pertains to
- A crime reference number if relevant
- The incident to which the footage relates
- The operator who removed the footage
- The person who holds the footage

As per [Property and Exhibits Procedure](#) the person who holds the footage at this point is responsible for maintaining its security and integrity in accordance with the [Review Retention Disposal of Information Procedure](#) as an exhibit under [MOPI Guidelines](#) and the [CPIA Code of Practice](#)

- 8.4. Disposal:** Data shall be retained on the system for a minimum 31 days after which it will be automatically overwritten by the system as per the above retention guidelines.

Where that data has been removed, its disposal is the responsibility of the Investigating Officer again in line with Review Retention Disposal of Information Procedure.

9. Access to the CCTV System

- 9.1.** Access to the CCTV system is restricted to authorised personnel only. This includes designated officers and staff whose roles require access for operational, investigative, or maintenance purposes. Access is granted based on role-based necessity and is subject to the following controls:

- **Access Assessment:** All personnel requesting access must undergo an assessment to determine the necessity and proportionality of access in line with their duties.
- **Training and Competency:** Individuals must complete mandatory training on data protection, system use, and relevant legislation (e.g., DPA 2018, RIPA) before access is granted.
- **Audit and Monitoring:** All access to the system is logged and subject to regular audits to ensure compliance with policy and legal requirements.
- **Revocation of Access:** Access rights are reviewed annually and may be revoked if no longer required or if misuse is identified.

10. Third Party Access Requests and Complaints

- 10.1.** The Freedom of Information Act 2000 gives the public a general right of access to information held by local authorities to promote openness and accountability. This Act may be used to request specific information about the operation of the system.

However due to its sensitive nature, recorded material collected by the system is not usually available under this Act. The material will usually contain personal data and this is usually exempt from disclosure under the Act. Individuals are advised to seek access via the Data Subject Access legislation in the Data Protection law if they require access to recorded material that relates to them.

11. Data Subject Access Request

- 11.1.** Section 45 of **The Data Protection Act 2018** and Article 15 of the General Data Protection Regulation (GDPR) gives provision to individuals to request access to information held about themselves. This provision means that a person may make a request to the data controller who will task the system manager to view and retrieve a copy of footage of the person making the request which has been captured by The System.

- 11.2.** A person making a request to review footage of themselves can do so through a Subject Access Request made under the Data Protection law:

Request information about yourself or someone else – Subject Access Request Form.

[Subject Access Procedure](#): Such requests should be made to the Civil Disclosure Unit, who will retrieve the requested information from the system operator.

12. Maintenance of the system

- 12.1.** The maintenance of the physical provision of the system is the responsibility of the Estates Department which is encapsulated in a maintenance contract. This remains in place for the life of the contract, which ensures that the hardware, software and system are kept continually secure, maintained and updated. A regular audit/service of the system will be undertaken a minimum of annually to ensure the recorders are working appropriately and retaining data for 31 days and that cameras remain proportionate to the need.

13. Legislation

- 13.1.** The operation of the System has been notified to the Information Commissioners Office (ICO).
- 13.2.** The system has been installed, operated and managed in accordance with [ICO's Video Surveillance Guidance](#) which enables North Yorkshire Police to demonstrate to communities and staff that we are operating best practices which are transparent and proportionate.

- 13.3. The cameras will be checked on an annual basis to assess their proportionality and that they are justifiable to meet the objectives.
- 13.4. This Code of Practice also takes into consideration the [College of Policing Practical Advice on Police use of Digital Images](#).
- 13.5. General police practices further ensure that the system complies with the following legislation:
- Data Protection Act 2018
 - The Regulation of Investigatory Powers Act 2000
 - Police and Criminal Evidence Act 1984
 - Health and Safety at Work Act 1974
 - Crime and Disorder Act 1998
 - Human Rights Act 1998
 - [Protection of Freedoms Act 2012](#)
- 13.6. Requests for disclosure of CCTV images for use in evidence must be processed in accordance with the requirements of the Criminal Procedures and Investigation Act 1996 and its Codes of Practice. Retention periods for images served under these circumstances will be as for all viewed material. Evidence will be stored in accordance with MOPI guidelines as detailed above.
- 13.7. The **Regulation of Investigatory Powers Act 2000 (RIPA)** was introduced to regulate surveillance and similar activities carried out by public bodies. The system will be used primarily for overt capture of data. The CCTV operators shall be trained to identify surveillance that requires RIP Act authorisation and know the process required to obtain this authorisation. Surveillance requiring such authorisation shall not be carried out without obtaining authorisation. Certain instances may necessitate retrospective authorisation.

The Act defines two types of covert surveillance relevant to the use of CCTV systems, “intrusive” and “directed” surveillance. The system shall not be used for these purposes unless authorised under RIPA to be done so. Operators will be trained in this Act and have a good level of understanding of what constitutes intrusive or directed surveillance.

14. Equality and Privacy Analysis

- 14.1. An **Equality Analysis** will be completed, that identifies any potential impact of the proposal on each of the following protected groups:
- Disability
 - Age
 - Sex
 - Sexual Orientation
 - Gender reassignment
 - Marriage and civil partnership
 - Pregnancy and maternity
 - Race
 - Religion

14.2. A Privacy Impact Assessment will be completed overarching the general aims specific to the type of use of the camera.

Privacy Impact Assessments: Every consideration will be given to the right of the general public to go about their daily business with minimum loss of privacy. Whereas total privacy cannot be guaranteed within a CCTV surveillance area, the cameras will not be used to unduly monitor persons going about their lawful business. It is inevitable that individuals could be caught on camera briefly during general surveillance, but persons will only be specifically monitored, for any length of time, if there is suspicion or knowledge that an incident may have occurred or be about to occur.

15. CCTV System Review

15.1. Compliance with the Information Commissioner's Code of Practice and The Surveillance Camera Code of Practice will result in an annual audit and review of the CCTV system to ensure:

- that the cameras remain justified and proportionate, fit for purpose and function
- that the scheme is still necessary and effective in achieving the purposes outlined in the Code of Practice or in the individual policies held

16. Code of Practice Review

16.1. The Code of Practice will be reviewed every 3 years or sooner if new legislation/guidance, which may have an impact, is introduced. The Code of Practice may also be reviewed should the above system review result in required changes. The strategic lead will be responsible for reviewing this.

17. Public Information

17.1. Publication: A copy of this Code of Practice shall be published on North Yorkshire Police website, the Policies and Procedures Intranet Subsite, the CCTV Force Intranet subsite (hyperlink creations) and a copy will be made available to anyone on request.

17.2. Signage: This will be placed in the locality of the cameras and at main entrance points to the relevant area. The signs will indicate if required:

- The presence of CCTV monitoring
- The 'ownership' of the system and name of 'Data Controller' of the system
- Contact telephone number of the Data Protection Officer/information about the System

17.3. Cameras capable of obtaining personal information from private property will not be used to do so except under the specific requirements of a Regulation of Investigatory Powers Act (RIPA) request (see section 9.1). Furthermore, such a

RIPA request will only be made for investigations originating from the police or other body investigating serious offences. Minor and non-criminal offences will not be investigated using intrusive surveillance.

18. Definition of Special Terms

- 18.1. CCTV** - Closed Circuit Television (CCTV) is technology which provides an effective means of identifying people, vehicles or incidents that may result in action being required by Police or partner organisations. It is a proactive policing tool for investigations which can help prevent criminality by targeting areas which are subject to higher levels of crime and anti-social behaviour or at risk of security breach.
- 18.2. Data Controller** - The Chief Constable is the Data Controller for the CCTV systems operated within North Yorkshire Police. As such they have responsibility for compliance with DP law. This CCTV Code of Practice is the overall responsibility of the Chief Officer with Estates oversight.
- 18.3. The System** - Refers to the surveillance system installed within North Yorkshire Police Buildings or buildings where Chief Constable Personnel and the functions provided by the Police and Crime Commissioner are based.

19. Acronyms

- **CoP** - College of Policing
- **APP** – Authorised Professional Practice
- **DPA** – Data Protection Act 2018
- **RIPA** – Regulation of Investigatory Powers Act 2000
- **FOIA** –Freedom of Information Act 2000
- **ICO** – Information Commissioners Office
- **MOPI** – Management of Police Information

20. Linkages

20.1. Subsidiary Linked Procedures:

- [Property and Exhibits Procedure](#)
- [Review, Retention and Disposal of Information Procedure](#)
- [Records Management Policy](#)
- [APP-Detention and Custody-CCTV](#)
- [CCTV in Custody Procedure](#)
- [Information Security Policy](#)
- [Physical Security Procedure](#)

20.2. Other Documents:

- [CCTV Code of Practice – ICO](#)
- [Value of CCTV in Investigations 2017](#)
- [National surveillance camera strategy for England and Wales](#)

CCTV – NYP estates mounted CCTV Codes of Practice Policy

- [Steps to complying with the 12 principles](#)
- [Surveillance camera code of practice](#)