

**Data Protection Impact Assessment**

**CLOSED CIRCUIT TELEVISION (CCTV)**

|  |  |
| --- | --- |
| Completed by: | Ann Hardacre, CCTV Manager  |
| Information Asset Owner:  | Head of ICT  |
| Division / Department:  | ICT Department, Headquarters  |
| Date Completed: | 20th May 2022. Reviewed November 2023  |
| Review Date: | December 2024 |

# THE REQUIREMENT FOR THE [*INSERT SYSTEM/ PROJECT/ INITIAVE/ POLICY]*

Insert brief details regarding the proposal Overview of the new system / process, change to existing system or new use of personal data

What do you want to achieve from the proposal and how will your plans for processing personal data help to achieve your purpose?

Clearly state your objective/ Provide evidence for why the proposal is necessary. The evidence can consist of facts, statistics, reports etc.

Describe why existing and/or less intrusive measures would be inadequate. Would any less intrusive options would achieve the same goal. Are there existing processes or techniques could be used instead of new intrusive measures.

Lancashire Constabulary has Closed Circuit Television (CCTV) on Constabulary premises for several years. The system is provided by AJAR Technhology, and the organisation has 174 external cameras and 94 internal cameras located across Lancashire.

The purpose of the CCTV system is for monitoring of security in areas and premises used by staff and members of the public to maintain the safety of those who work within or visit the Constabulary and to enable the prevention, investigation and detection of crime, apprehension, and prosecution of offenders.

Milestone is a Video Management System (VMS) which manages the recording, management and storage of all CCTV data within the station environment in a central secure way.

The Digital Evidence Management System, NICE Investigate will remove the need to produce discs as all footage will be stored digitally. This is aimed to expedite the sharing of evidence to aid investigations and reduce the risk/prevent any loss of data from misplaced evidence.

This Data Protection Impact Assessment has been written to explain:

* The rationale for Lancashire Constabulary continued and extended use of this technology
* The legality behind its use
* The key privacy issues and risks, risks and provides an explanation as to how the organisation mitigates them.
* How the Constabulary will continue to monitor the use of the equipment, together with responding to any national and legislative changes
* How data is stored and transferred for evidential purposes
* To ensure compliance with Surveillance Camera Code of Practice, Data Protection regulations and relevant legislation

# IDENTIFY THE NEED FOR A DPIA

Summarise why you identified the need for a DPIA. The [DPIA Screening document](https://collaboration.lancres.lancashire.police.cjx.gov.uk/sites/legal-services/DPO/_layouts/15/WopiFrame.aspx?sourcedoc=%7b591B85E7-1591-486C-A757-AA74CFF60F5C%7d&file=DPIA%20screening%20form.docx&action=default) will inform this section if it has been completed. If you have completed one, reference so here.

If not, summarise why you identified the need for a DPIA, eg volume/ sensitivity of personal data, new technology, etc.

You may find it helpful to refer or link to other documents, such as a project proposal.

The Data Protection Impact Assessment is required to achieve compliance with the Surveillance Camera Code of Practice and data protection legislation.

The closed-circuit television is provided by AJAR Technhology. The accompanying software is called Milestone. Milestone is a Video Management System (VMS) which manages the recording, management, and storage of all CCTV data within the station environment in a central secure way.

A requirement for a DPIA has been identified which acknowledged that the CCTV system will be capturing the personal data of a large number of individuals on a daily basis and may be used for a law enforcement purpose.

The CCTV system operates through a serious of fixed cameras installed throughout the county. The CCTV is recorded onto a hard disc drive called the Milestone platform.

Data is processed when a request is submitted on the ICT portal. A member of trained staff transfers the requested data onto the Milestone platform then onto the forces secure network server. The data is then uploaded onto the NICE Investigate portal.

The digital recorder stores footage for 31 days after which time old data is overwritten with new i.e. the maximum recorded data will never exceed 31 days.

# A DESCRIPTION OF THE PROCESSING TO BE UNDERTAKEN

Consider each of the following questions. These seek to establish the processing lifecycle. Where appropriate it may be helpful to create a data flow diagram.

The CCTV system is an essential tool used by Lancashire Constabulary for monitoring of security in areas and premises used by staff and members of the public to maintain the safety of those who work within or visit the Constabulary and to enable the prevention, investigation and detection of crime, apprehension, and prosecution of offenders.

The CCTV system operates through a serious of fixed cameras installed throughout the Lancashire area. The CCTV is recorded onto a hard disc drive called the Milestone platform.

## What is the purpose of the processing?

Is use compatible with the original purpose or is this a new purpose?

Are new purposes likely to be identified as the project progresses / scope expands

The CCTV fixed cameras which are located throughout the county have the ability to capture visual recordings in high definition. These cameras capture identifiable images of individuals and vehicles passing to, from and within the perimeter and egress points. This system is only used by staff trained in its use.

Processing is used for its original purpose. We use it for identifying offenders or incidents that has occurred on Constabulary premises based on a criminal nature.

There will be collateral intrusion involving other persons involved but also those persons who are not. The camera may also capture information not relevant to the incident in question for example an individual at an enquiry desk being dealt with by another member of staff or member of the public walking past Constabulary premises.

There may be occasions where the CCTV supplier is required to have access to the data held on the system for support purposes. This would largely be in relation to audit carrying out routine maintenance or fixing a fault on the system rather than actual footage. This could either be via remote access using the standard process or through the supplier attending Constabulary premises. Any person working on the system will be vetted.

The CCTV footage that is downloaded will be kept in accordance with Lancashire Constabulary retention schedule and storage policy.

## How is data collected?

What steps can be taken to ensure data quality.

Mandatory / optional data fields.

The CCTV system is running continuously on Constabulary premises.

Information is captured via a network IP camera which transfers the feed over the camera network back to the local server.

The data is processed via Milestone platform onto the local hard drives.

Footage can be played back to identify the incident via the Milestone platform on any network computer or encrypted Constabulary laptop. The Digital Evidence Management system, NICE Investigate is then used to retrieve and download the relevant footage off the system for evidential purposes.

Non-evidential data will be auto deleted by the Milestone platform after 31 days as stated in the Premises Security CCTV Policy. Footage required as evidential will then be downloaded onto NICE Investigate.

The data quality rescheme is currently under review an issues report is currently with the Senior Management Team for consideration. The intended process will allow our Force to test the CCTV system on a regular basis to make sure each camera is working and carry out a cleaning regime three times a year for our external cameras that are exposed to the elements i.e. car fumes, grit, spider’s webs, and sand.

On an annual basis our supplier carries out a planned preventive maintenance (PPM) visit which is part of the maintenance contract. From the visit a comprehensive report is completed and reviewed, if any anomalies are identified this would then be reported to the Overt Surveillance Governance Board.

## How is data processed?

Data is processed when a request is submitted on the ICT portal. A member of trained staff transfers the request data onto the Milestone platform then onto the forces secure network server. The data is then uploaded onto the NICE Investigate portal. This is governed by the Criminal Procedure and Investigations Act 1996 (CPIA) which sets guidelines for how police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation and which may be relevant to the investigation and related matters.

## How is data stored?

Electronic / manual records / On-site / off site etc

Data is stored on the Milestone Platform with local backup storage at a second location if marked as evidential it is retained in NICE investigate. If not, it is deleted in 31 days.

Footage ingested into the NICE Investigate is stored in Microsoft Azure and retained in line with MOPI rules which will be implemented by the Digital Evidence

Management system.

The server onsite in the server room or PABX which is secured with a key which at present some of these rooms are moving onto access control where access can be even more limited.

## How is data used?

Can the data be anonymised?

Data may be used for evidential purposes. It might be used in other circumstances e.g. misconduct investigations were lawful and necessary. Presently, force policy does not allow for the use of damage to personal property.

## Who has access to the data?

Is there appropriate access control in place / how will the ‘need to know’ principle be enforced?

Authorised personnel i.e. ICT department have access to the data, this is monitored through the auditing process. This is all down to access credentials.

## Will the data be shared?

Is this sharing compatible with the purpose?

Does the processing involve sharing / disclosure to external partners?

Other organisations with which CCTV may be shared include the Crown Prosecution Service, Legal Representatives, and the Independent Office for Police Conduct (IOPC). Any images released to those organisations will be authorised for the lawful purpose and limited to that which is necessary.

Facilitation of the data sharing will be managed by the use of secure passwords and links to the system which only give access to the data required. There is no threat to access being granted by outside agencies to data not applicable to their incident/investigation.

Digital Evidence would be uploaded to NICE investigate collated into NICE Investigate case and shared with CPS via the NICE Investigate sharing portal that provides a URL link that will enable CPS to view and download the evidence.

The data may be shared via the secure network NICE as previous stated.

## Are processors used?

Is a Data processor contract in place or will it need to be established.

Where the data be held UK / EUROPE / WORLDWIDE

Edesix as the service supplier will be a processor of personal data in relation to the support services. The support will be via Webex and manged by ICT as the solution is hosted on Lancashire servers therefore no Edesix support will be provided unsupervised.

The necessary data processor contract terms are established with Edesix.

The data will be held in the UK.

## What are the retention periods?

How long does this data need to be held to achieve the purpose? Is this documented?

Does all of it need to be kept for all of the time? Does the [Force Retention Schedule](https://documents.lancres.lancashire.police.cjx.gov.uk/_layouts/15/WopiFrame.aspx?sourcedoc=%7b10EF920C-CF99-4E13-A07E-47103F9493EF%7d&file=Lancashire%20Constabulary%20Retention%20Schedule.docx&action=default&DefaultItemOpen=1) need to be updated?

CCTV data is retained for 31 days, this is captured within the Premises Security CCTV Policy.

The digital recorder stores footage for 31 days after which time old data is overwritten with new i.e. the maximum recorded data will never exceed 31 days.

## How will data be deleted?

How will retention and disposal be managed securely? Can this be automated? How will reviews be flagged?

The data is automatically overwritten after the 31 days. The retention is managed automatically by the servers. If a problem ever occurs with the hard drive this will be shredded.

## What security measures are in place?

Has consultation been undertaken with the Information Security Officer?

What is the security classification of personal data to be processed?

Has an information security assessment of the processing taken place?

It is an on-premises solution, and we hold the data in our data centre therefore the system and data will be protected by all the usual Constabulary security measures such as antimalware, firewalls and lock down policies for the servers. This is also managed by access control and only vetted members of staff can access the system.

Consultation has been carried out with the Information Security Officer. The security classification is official classification.

CCTV is subject to due diligence by Information Security to ensure we meet the Force requirements in respect of (security measures) cyber security. Any system that is accessible through the Force network is required to meet the Codes of Connection for PSN and PSNP accreditation. A pen test was carried out in 2018.

## Are any new technologies in use?

No

## Logging and categorisation

Does the system maintain an audit trail of transactions to assist with investigating instances of system misuse?

The categories of personal data that are collect includes video and photographic images of police officers, police staff and members of the public entering police premises also vehicles entering or passing the premises.
The system is auditable to ascertain who may have accessed/actioned the system at any given time.

# THE SCOPE OF THE PROCESSING

## What is the nature of the data?

Does it include special category or criminal offence data?

Premises CCTV captures interactions between police officer, police staff and members of the public in visual format. The content of footage will vary but could contain an incident linked to criminal damage or assault.

Additionally, there will be collateral intrusion involving other persons involved, but also those persons who are not.  The cameras may capture information not relevant to the incident in question.

## What is the volume and variety of the data?

The below is a table of how many CCTV cameras are located on Constabulary premises, both external and internal.

|  |  |  |
| --- | --- | --- |
| **LOCATION** | **EXTERNAL** | **INTERNAL** |
| East Division  | 44 | 23 |
| West Division  | 34 | 31 |
| South Division  | 49 | 16 |
| Headquarters  | 47 | 24 |

The data will capture routine coming and going from and within Constabulary premises.

## What might be the sensitivity of the personal data?

Consider for example Victims / Witnesses / Children / health data

During the installation of the CCTV safeguarding were put in place to reduce privacy intrusion.

A privacy masking was included to local business and private property.

Footage is likely to be captured of all people including police officer, police staff and members of the public who have a legitimate purpose to be within police premises and going about their role. The subjects may be of any age, gender, and ethnicity.

## What is the duration of the processing?

Footage will be collected 24 hours a day, 7 days a week. This is continuously saving the data.

The digital evidence will be uploaded into NICE Investigate for the duration of the associated investigation and will be retained in line with retention schedules and relevant legislation.

## What is the number of data subjects involved and what is the geographical area covered?

Subjects within the area boundary of Lancashire Constabulary will be covered.

# THE CONTEXT OF THE PROCESSING

## The Source of the data

Members of the public/ Force systems / external systems

The source of the data will come from the CCTV recording. The subjects of the footage could be any person or vehicle.

## The nature of your relationship with the individuals?

Police officers, police staff and members of the public who have a legitimate purpose.

Collateral intrusion, it is inevitable that some members of the public will be filmed whilst legitimately going about their business.

## The extent to which individuals have control over their data?

If processing based on consent, can consent be withdrawn?

Individuals will be able to exercise their right to access to the data should they wish. Privacy notices are located around Constabulary premises, providing contact details for the Data Controller. A specific privacy notice relating to site CCTV will be published on the Constabulary website.

## The extent to which individuals are likely to expect the processing?

Have fair processing requirements been addressed?

The force privacy notice explains what personal requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

The footage will be redacted where appropriate to negate the unnecessary processing of personal data.

A specific privacy notice relating to CCTV has also been published on the Force website.

Individuals involved in the associated crime investigation should have an expectation that any digital evidence that appear to be shared with CPS.

## Whether they include children or other vulnerable people?

It will not be possible to prevent data being taken from children and vulnerable people, but as indicated footage can be redacted if the subject is not required as part of the investigation.

## Any previous experience of this type of processing?

CCTV is not new to Lancashire Constabulary or to the public service. There is now a fairly common understanding by members of the public the benefits of CCTV.

## Any relevant advances in technology or security?

No

## Any current issues of public concern?

The public would expect the police to be open and transparent by openly displaying how we use our CCTV, this is demonstrated through supporting documentation i.e. privacy notice, self-assessment tool, DPIA and signage that is clearly displayed on Constabulary premises that states who operates the system and include a point of contact for further information.

## Lancashire Constabulary takes account of and seeks to adhere to the 12 principles of the Surveillance Camera, Code of Practice.

## Have you considered and complied with any relevant codes of practice?

Surveillance Camera Code of Practice.

# DESCRIBE THE PURPOSE OF THE PROCESING

## The intended outcome for individuals.

The processing is designed to ensure:

* The security, health and safety of police officers, police staff, members of the public, police premises and other police assets.
* To prevent, deter and if necessary, support the investigation of unauthorised access, damage to secure premises, IT infrastructure or operational information.
* Assist in the prevention, detection and investigation of theft or other criminal offences.
* To assist in internal disciplinary investigations, where proportionate and appropriate to do so.
* Assist in the handling of insurance matters/claims.

Other individuals may also come into contact with the Police CCTV systems such as employees of companies either directly or indirectly dealing with or trading with Lancashire Constabulary.

Lancashire Constabulary will use the minimum amount of personnel information necessary to carry out a particular activity.

## The expected benefits for a society as a whole?

There are several benefits to society as a whole, these are:

* Help facilitate and protect the ability to provide a police service to the public
* Prevention and detection of crime
* Apprehension and prosecution of offenders
* Enhance the safety of the Public and our Police Officers and Police Staff
* Release operational efficiencies
* Maintenance of law and order
* Protection of property and the public purse
* Deterring anti-social behaviors
* Public Safety

CCTV when used proportionately and lawful is an effective tool to gather primary and supportive evidence in detection and investigation of crime. Assist in the tracking and apprehension of persons who are suspected of having committed a criminal offence. Assist in the identifying of witnesses. It can also be used to assist with the co-ordination of major events for public safety.

# CONSULTATION

## Describe when and how you will seek individuals’ views?

*(Any new/ changes in Policy may be subject to the formal consideration via the procedures relating to corporate policies.)*

Site CCTV has been in operation for some time and prior to the requirement to undertake data protection impact assessments. There is a common understanding that such technology would be used to protect any government or public buildings from damage or intrusion.

There is an Overt Surveillance Governance Board which comprises of key stakeholders i.e. asset owners, ICT, Estates, Data Protection, Information Security, and Divisional representation who come together on a quarterly basis and discuss all areas linked to Overt Surveillance.

Monthly meetings are held with our supplier to discuss all areas linked to CCTV.

Consultation has previously been undertaken as follows.

A site CCTV policy is to be produced which will be subject to the corporate policy consultation process.

| Who | When | How | Outcome  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Do you plan to consult information security experts, or any other experts?

The Information Security Officer has been consulted along with the Data Protection Manager.

# NECESSITY AND PROPORTIONALITY

## Lawful Basis for Processing

*What is the lawful basis for processing; which conditions for processing are met? If special category personal data is processed an additional lawful basis is required. Is the processing for law enforcement purposes (as opposed to general processing).*

*The Data Protection Office will be able to assist in identifying the correct legal basses relied upon for processing.*

General processing will be undertaken on the lawful basis:
 GDPR 2016 Article 6(e) – the processing is necessary for the performance of a task
 carried out in the pub interest.

When processing is undertaken on the grounds of public interest, the necessity for processing will arise from the exercise of a function conferred on a person by an enactment or rule of law. (Section 8 (c) Data Protection Act 2018). Such functions may be identified from common law policing powers and the following statutory provisions:

Section 39A of the Police Act 1996 requires Chief Officers to give “due regard” to statutory codes. The statutory Code of Practice relating to the Management of Police Information (MOPI) sets out the policing purposes as:

* protecting life and property,
* preserving order,
* preventing the commission of offences,
* bringing offenders to justice, and
* any duty or responsibility of the police arising from common or statute law.

Further, the Police Reform and Social Responsibility Act 2011, Sch 2. (7) provides that a Chief Constable may do anything which is calculated to facilitate, or is conducive to, the exercise of the functions of a Chief Constable, the delivery of efficient and effective policing, and managing complaints.

Other relevant legislative provisions where general processing might take place include but are not limited to:

The Civil Contingencies Act 2004

 The Crime and Disorder Act 1998

 The Policing Protocol Order 2011

Should general processing include the capture of a special category of personal data, which is defined at Article 9 of GDPR as data revealing:

* + racial or ethnic origin
	+ political opinions
	+ religious or philosophical beliefs
	+ trade union membership
	+ genetic data, biometric data
	+ data concerning a natural person’s sex life or sexual orientation

Law enforcement processing will be undertaken on the basis that it meets one of the conditions set out at Schedule 8 of the Data Protection Act 2018, namely:

* + a function conferred by an enactment or rule of law, necessary in the substantial public interest
	+ the administration of justice
	+ the safeguarding children and individuals at risk

General processing will be undertaken in accordance with the condition set out at Article 9(g), substantial public interest on the basis of law, where one of the following conditions from Part 2, Schedule 1 is met:

* prevention/ detection of unlawful acts
* protecting the public against dishonesty
* regulatory activity
* safeguarding of children and adults at risk

As a competent authority Lancashire Constabulary will collect data for the purpose of law enforcement, which are defined at Section 31 of the Data Protection Act 2018, as:
 “the prevention, investigation, detection or prosecution of criminal offences or the
 execution of criminal penalties, including the safeguarding against and the prevention
 against and the prevention of threats to pubic security’.

## Does the processing help to achieve a purpose?

Yes, the footage provides evidence in a criminal investigation.

It may on occasions be used for other purposes where lawful basis has clearly been established and it is proportionate to do so, this may include misconduct investigations or investigations operated by the IOPC.

## Is there another way to achieve the same outcome?

No

## How will you prevent function creep?

The Asset Owner is required to monitor and oversee the purposes for which the system will be used. There is no function creep.

## How will you ensure data quality, minimisation, and consistency?

The footage is date and time stamped so you know exactly when the footage has been retrieved.

The milestone system watermarks all images to ensure that the footage cannot be tampered with.

Footage for CCTV on Constabulary premises is only presently shared if it is linked to a criminal nature. This is captured within the premises and security CCTV policy.

## Data retention?

*Will data be stored in accordance with the* [*Force Retention Schedule*](https://documents.lancres.lancashire.police.cjx.gov.uk/_layouts/15/WopiFrame2.aspx?sourcedoc=%7b10EF920C-CF99-4E13-A07E-47103F9493EF%7d&file=Lancashire%20Constabulary%20Retention%20Schedule.docx&action=default&DefaultItemOpen=1)*?*

All data is stored in accordance with the Premises Security CCTV policy and the Force Retention Schedule.

## How do you intend to provide privacy information to individuals?

*See guidance on intranet regarding* [*Privacy Notices*](https://documents.lancres.lancashire.police.cjx.gov.uk/_layouts/15/WopiFrame.aspx?sourcedoc=%7b2006E6DF-609E-45AB-8C5A-D10F22D69A6B%7d&file=Specific%20Privacy%20Notice%20Template.docx&action=default&DefaultItemOpen=1)*.*

The Privacy Notice has been published on Lancashire Constabulary website for members of the public to view.

Signage is clearly displayed on Constabulary premises inside and outside of the premises, this states who operates the system and include a point of contact for further information.

## How will you help implement and support individual’s rights (access / erasure / rectification)?

This DPIA has been conducted to identify privacy concerns and to address those with agreed mitigation actions being incorporated into the project. Personal data can be extracted from Milestone and Nice Investigate for the purpose of fulfilling data subject’s rights requests and can manually delete if a right to erasure was approved. Individuals will be provided with privacy information via the Force privacy policy and the NICE privacy policy.

## How will you safeguarding access to the system / data?

This system is password protected. Access to the system is managed by identified users, which come from Lancashire’s Active Directory and use single sign on.

The milestone system watermarks all images to ensure that the footage cannot be tampered with.

## How will the system and processing be audited?

The system has full auditing functionality on Milestone and the Information Asset Owner will undertake period monitoring.

We currently don’t undertake auditing this will be part of the testing and auditing regime, once staff are in place.

# RISK ASSESSMENT

*A copy of the full risk assessment should be completed and attached as an Appendix.*

*(The* [*Risk Assessment Template*](https://collaboration.lancres.lancashire.police.cjx.gov.uk/sites/legal-services/DPO/_layouts/15/WopiFrame.aspx?sourcedoc=%7b46E6C5B8-914A-4797-A419-9FE49B4B6F8A%7d&file=DPIA%20template%202019%20Appendix%20risk%20assessment.docx&action=default) *for this can be found on our intranet site).*

The use and operation of CCTV for the protection of Constabulary premises, staff and visitors whilst on-site has been in operation for a number of years. During the completion of this DPIA no residual risks have been identified.

# SIGN OFF AND OUTCOMES

|  |  |  |  |
| --- | --- | --- | --- |
|  | Name  | Date  | Notes |
| Submitted to the Data Protection Officer (DPO) for views by author: |  |  |  |
| DPO Advice provided by :  |  |  |  |
| DPO Advice / Comments: | The DPIA has covered the relevant issues relating to the use of CCTV on site. Individual assessments are conducted of specific sites to ensure privacy risks are minimised, e.g. to neighbouring properties. Information security risks have been assessed and are managed appropriately. It is noted that in the foreseeable future a Site CCTV Policy is to be considered.  |
| DPO Signed off: | Carl Melling  | 29/11/23 |  |
| Information Asset Owner (IAO) signed off:  |  |  |  |
| IAO Comments: |  |
| Reported to Information Governance Board: |  |
| Monitoring/ Update :  |  |