Northamptonshire Police

CCTV on Police Premises Policy

Policy Owner: Deputy Chief Constable
Department Responsible: Enabling Services
Chief Officer Approval: Deputy Chief Constable
Date of Next Review: May 2023
Review log: Initial Policy Document. V1.2
Section Author: David McInally
Date of current version: May 2022

CCTV (Police Premises) Policy November 2019

1. Statement

This policy relates to the use of overt closed circuit television (CCTV) on police premises (and mobile police stations) as a security and crime prevention measure. This policy is not intended to cover the use of CCTV in any other setting or for any other use.

The Information Commissioner's Office (ICO) issued its first code of practice under the Data Protection Act 1998 (DPA) covering the use of CCTV ('the code') in 2000 (updated in 2015).

The Code was developed to explain the legal requirements operators of surveillance cameras (CCTV) were required to meet under the DPA and promote best practice. The Code also addressed the inconsistent standards adopted across different sectors at that time and the growing public concern caused by the increasing unregulated use of CCTV and other types of surveillance cameras.

Further legal, practical and technological developments connected to CCTV usage, such as Automatic Number Plate Recognition (ANPR) and Body Worn Video (BWV) means that reviews of the Code have been, and continue to be, necessary. CCTV cameras are no longer a passive technology that only records and retains images, but is now a proactive technology that can be used to identify people of interest and keep detailed records of people's activities. The use of CCTV in this way has aroused public concern due to the technology no longer being used solely to keep people and their property safe, but increasingly being used to collect evidence to inform other decisions.

The unwarranted use of CCTV and other forms of surveillance cameras has led to a strengthening of the regulatory landscape through the passing of the Protection of Freedoms Act 2012 (POFA). The POFA has seen the introduction of a new surveillance camera code of practice issued by the Secretary of State since June 2013 and the appointment of a Surveillance Camera Commissioner to promote the Code and review its operation and impact.

There is therefore a tougher regulatory landscape involving enforcement action restricting the unwarranted and excessive use of surveillance. The data protection implications of using CCTV and other forms of surveillance cameras are real and the Police need to ensure compliance in the use of our own CCTV equipment.

2. Aims

To ensure Northamptonshire Police is compliant with appropriate legislation and best practice surrounding the use and processing of information (including personal and sensitive personal information) captured by the CCTV in and around its buildings and Estate.

To achieve this aim, the use and processing of information of CCTV must be:

Proportionate: it must be fair and achieve a balance between the needs of society and the rights of the individual.

Legal: it must be conducted correctly and legitimately in accordance with the relevant Data Protection legislation, Information Commissioners Office (ICO) Code, Human Rights Act 1998 (HRA) and Common Law Duty of Confidence and Freedom of Information legislation (FOI). Privacy impact must be considered.

Accountable: its use must carried out in accordance with the above legislation and code's.

Necessary: it must be justifiable based on the threat and risk presented at the time required and at each review.

Best: it must be made against the best information reasonably available at the time and reviewed regularly to ensure continued relevance and compliance with the above legislation and codes.

3. Scope

This policy relates to the use of, and the processing of information (including personal and sensitive personal information) captured Northamptonshire Police in and around its buildings and estate. This policy does relate to CCTV used within police custody suites, and mobile police stations but not to CCTV used in a covert manner (this is the subject of Regulation of Investigatory Powers Act 2000) and is cognisant and compliant with the following:

Data Protection Act 1998
Human Rights Act 1998
Freedom of Information Act 2000
Protection of Freedoms Act 2012
Information Commissioner's Code 2015

The scope of the system is to act as a visible deterrent, but then to be of sufficient calibre to capture images and audio (where applicable) to assess the incident and to support criminal or civil cases. Part of that strategy is to advertise the systems presence.

The system in consultation with Counter Terrorism Security Advisors and crime prevention officers covers key areas of Police Estates that would be of interest to those with criminal intent. The systems are limited to capturing data related to policing premises only (static and mobile). This will be in terms of perimeter boundary/internal grounds security and high risk areas within premises. The high risk areas include: Custody suites, property stores, armouries, unoccupied remote sites and enquiry desks.

For unoccupied remote or non 24/7 sites, the CCTV system will be linked to intrusion alarms which will provide live time warning of an incident, affording the Force Control Room to view and risk assess the incident.

The intention long term is that all Police sites have a system that feeds into the central function allowing access to key personnel to make live time

decision relating to intrusions on Police Estates and therefore deploying a proportionate response.

This is quite a sophisticated and advanced use of CCTV and alarms. There is no apparent future development capability to protect Police Estate and those working in Police Estate.

Any other use of this technology beyond the scope of the activity within this document must be subject to further policy for the purpose being proposed.

4. Legal Basis

To ensure Northamptonshire Police treat its personnel and the public captured by our CCTV systems fairly, lawfully and in line with the scope of this procedure, the installation and use of CCTV on police premises will abide by the ICO Code and DPA principles detailed later in this document.

The DPA not only creates obligations for organisations processing personal and sensitive personal information, it also gives individuals rights, such as access to their personal information and to claim compensation when they suffer damage or distress.

The basic legal requirement is to comply with the DPA itself. The ICO's code advises on how the legal requirements of the DPA can be met.

The Code also reflects on the wider regulatory environment. When using, or intending to use CCTV systems to help secure police premises, Northamptonshire Police need to consider their obligations in relation to the Freedom of Information Act 2000 (FOIA), the Human Rights Act 1998 (HRA), the Protection of Freedoms Act 2012 (POFA) and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (POFA code).

The POFA in particular has an important role in regulating surveillance systems alongside the DPA. It provides advice and guidance on issues such as operational requirements, technical standards and the effectiveness of the systems available. The following 12 guiding principles are the key component of the POFA code:

1. Use of 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 use 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. Signage is provided on every building with a system.

4. There must be clear responsibility and accountability for all surveillance camera

system activities including images and information collected, held and used. All requests for access to system data is requested through one source, with verification of the purpose of the data and audit trails of every request. Live access to data is restricted to functions who require live data in order meet 1 above.

FCR: live access to assess risk and threats to property and people in relation to live intrusions at Police premises. Building alarm systems will notify FCR of intrusions including a snap shot of CCTV coverage of the intrusion. FCR will then select live access to CCTV for the purpose of assessment and deployment of appropriate resources.

Enquiry Desk staff: access to live data streams for the purpose of security and identification of visitors at building locations where remote access can be granted upon verification of identity of the visitor.

Estates and Facilities personnel: access to live data for the purpose of reviewing security occurrences or incidents.

Security advisors: access to live data as part of the evaluation and review of security systems.

Custody staff: access to live and historical data pertinent to the operation of Custody Suites in order to protect Staff and detainees in line with operating procedures predetermined by EMCJS.

Information security personnel: to validate and verify information security including compliance to this policy.

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.

Images will be stored on a central storage database, with E-Forensics managing access to data. Official requests for data access including the purpose must be provided to gain access.

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.

As 6 above, all requests for historical data must be submitted in the approved manner and subject to verification and audit.

Data authorised will be sent in a sealed auditable manner or electronically to the requestor. An audit trail of data provided will be kept.

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.

4.1 Information Commissioners Office CCTV Code of Practice (May 2015)
Northamptonshire Police will make use of privacy impact assessments to ensure consideration and compliance is given to the above mentioned principles.

4.2 Governance
The Deputy Chief Constable of Northamptonshire Police is the Senior Information Risk Owner (SIRO) and is responsible for ensuring the processing of personal information is carried out in compliance with the DPA and as such is the strategic lead in respect of the management of CCTV images.

CCTV does however fall in to four distinct areas of business, ISD/E-Forensics (technical), Procurement (purchasing), Estates (maintenance) and Estates and facilities (policy and procedure).

Due to this the Assistant Chief Officer (Enabling Services) and the OPFCC will be involved in governance arrangements. They will be responsible for the monitoring and implementation of this policy and supporting process.

To ensure compliance with all appropriate legislation surrounding the use of and the processing of personal and sensitive personal information captures by CCTV on premises operated by the OPFCC / Northamptonshire Police the following information will be monitored:

□□Whether CCTV use is or continues to be lawful, justified, proportionate and necessary. This will incorporate the use of Privacy Impact Assessment and periodic reviews of the necessity of the relevant CCTV system, including location.

□□That there is clear responsibility and governance for the use of every CCTV system and the information that is recorded, retained and released. This will include ensuring that those involved in the use of CCTV are aware of their responsibilities, eg, signage.

4.3 Standard Operating Practices

The Northamptonshire Police, Fire and Crime Commissioner (PFCC) is responsible for commissioning and installation of CCTV. The Chief Constable of Northamptonshire Police retains ownership of the data captured by the CCTV and therefore the completion of the Privacy Impact Assessment (PIA). If a PIA was not completed prior to installation, a PIA will be completed by the premises asset owner. The PIA will be a living document and the subject of yearly reviews or sooner should there be any significant changes to the premises, CCTV system or other external factors, eg, building of new commercial or dwellings next to the police premise perimeter.

The assessment will be completed with the aid of a survey of the CCTV installation and site by the building asset owner, or their appointed representative. If deemed appropriate by the asset owner, a crime reduction office or Health and Safety advisor can assist.

A copy of the completed assessment will be retained at the premises for reference, and copy sent to the Policy Library.

This policy does not dictate a standardised retention period for the images or data captured by CCTV. As part of the PIA process, consideration will be given to a retention period that is proportionate, necessary and justified for the premise in question.

5. Review

This policy will be reviewed on a yearly basis to ensure it remains current and in line with developing legislation.

Appendix A

1. Procedure for the commissioning of new CCTV

The using of CCTV can be privacy intrusive as it is capable of putting law abiding people under surveillance and recording their daily movements. Consideration should therefore be carefully given regarding the use of such equipment. The fact that it is possible, affordable or has public support should not be the justification for its use alone.

When considering the installation of new CCTV the following should be addressed and documented:

The specific nature of the problem that we are seeking to address, eg, is it for the prevention or detection of crime or protection of the public and how

Is CCTV justified as an effective solution and how or are there better alternative solutions?

What effect will it have on individuals?

Is it a proportionate response to the problem?

Completion of a privacy impact assessment (PIA) is the most effective way to ensure that the above are covered and will be done in all cases (see appendix B). These will then be sent to the Information Management Department for recording.

2. Procedure for reviewing the continued use of CCTV

If a system is already being used it should be regularly evaluated as to its necessity and proportionality in line with procedure 1 above.

3. Procedure for reviewing and retaining CCTV images

It is essential to establish clear procedures relating to the processing of any personal information and how we handle and store information captured by CCTV is no different.
The force information manager has overall responsibility on behalf of the DCC for any information but it is important that at each location where we have CCTV there are:

Named individuals who have responsibility for the control of CCTV information and they manage, in conjunction with the information manager, what and how CCTV is recorded, stored, viewed and deleted at each location. This will need to be in compliance with legislation stated within the CCTV policy.

Methods to ensure that access to CCTV systems is restricted.

Clearly defined and specific purposes for the use of the CCTV which are communicated to all who have access and use it and clear records are kept for

the use.

Proactive checks or audits carried out on a regular basis to ensure that these procedures are being complied with an audit trail of this.

Appendix B

NORTHAMPTONSHIRE POLICE
CONDUCTING A PRIVACY IMPACT ASSESSMENT
GUIDANCE

Overview
A Privacy Impact Assessment (PIA) is a process which helps to assess privacy risks to individuals in the collection, use and disclosure of information.
PIAs help identify privacy and Data Protection compliance liabilities for the Force, foresee problems and bring forward solutions. The initiative can then be designed to avoid unnecessary privacy intrusion and features can be built in from the outset to reduce the associated risks and negative effects.
There is no statutory requirement for any organisation to complete a PIA; however, central government departments have been instructed to complete PIAs by Cabinet Office. The Information Commissioner's Office (ICO) has produced the PIA handbook, on which this guide is based, to help organisations assess privacy risks and liabilities.

The ICO recommends that organisations should conduct a PIA to: identify privacy risks to individuals, identify privacy and data protection liabilities for the Force, protect the Force's reputation, install public trust and confidence in the information sharing initiative, avoid expensive, inadequate 'bolt on' solutions, inform your communications strategy and enlightened self-belief.

The PIA should be conducted when: the initiative is being designed, you know what you want to do, you know how you want to do it and you know who else is involved, but ideally it should start before: decisions are set in stone, you have signed agreements and while you can still change your mind. Much of the work involved in conducting a PIA should formalise steps that should already be taken as part of the policy/ project development process and the wider impact assessment.

Responsibility for ensuing that the PIA is undertaken lies with the Senior Officer commissioning the initiative / project. Responsibility for undertaking the PIA rests with the System Owner / Project Manager.

Is a Privacy Impact Assessment necessary?
Not every project will require a PIA. The ICO envisages that PIAs should be used only where a project is of such a wide scope, or will use personal information, of such a nature, that there would be a genuine risk to the privacy of the individual. Examples of initiatives that may require PIAs could be new software installation, a new database only containing personal data of individuals, changes to retention policies relating to personal data.

Attached is an initial privacy impact assessment questionnaire series of questions that will help to determine whether a PIA is required. Where the answers to the questions are 'Yes', consideration should be given to the extent and scope of the

privacy impact and the resulting project risk. If only one or two aspects give rise to privacy concerns, the PIA process should be designed to focus on the areas of concern. If, on the other hand, multiple questions are answered 'Yes', a more comprehensive assessment is appropriate.

If it is deemed, a PIA is not necessary because the answers to series of questions are 'no', a record of the assessment being undertaken and the outcome should be recorded. If a PIA is required, a template adopted by Leicestershire Police is attached.

Please note that the PIA may form part of the Security Accreditation process. Further advice or guidance can be obtained from the Information Management Department.

NORTHAMPTONSHIRE POLICE
GUIDANCE ON CONDUCTING A PRIVACY IMPACT ASSESSMENT
Insert location name:
Insert PIA completion date:
SECTION (1)
NB: Complete this section first to establish if a privacy impact assessment is required
Is a Privacy Impact Assessment (PIA) required? YES ☒ NO ☒
If you are unsure as to whether a Privacy Impact Assessment is required, the following series of questions may help you to determine.
Where the answers to the questions are **'Yes'**, consideration should be given to the extent and scope of the privacy impact and the resulting project risk. If only one or two aspects give rise to privacy concerns, the PIA process should be designed to focus on the areas of concern. If, on the other hand, multiple questions are answered 'Yes', a more comprehensive assessment is appropriate.

Will the project involve the collection of new information about individuals?
Yes ☐ No ☐
Will the project compel individuals to provide information about them?
Yes ☐ No ☐
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
Yes ☐ No ☐
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
Yes ☐ No ☐
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
Yes ☐ No ☐
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
Yes ☐ No ☐

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
Yes ☐ No ☐
Will the project require you to contact individuals in ways which they may find intrusive?
Yes ☐ No ☐

PIA Code of Practice (51pg document)
Privacy Impact Assessments (PIAs)
Conducting a PIA is not a requirement of the Data Protection Act (DPA), but undertaking one will help to ensure a new project is compliant. The Information Commissioner's Office (ICO) encourages organisations to ensure privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:
□□building new IT systems for storing or accessing personal data;
□□developing legislation, policy or strategies that have privacy implications;
□□embarking on a data sharing initiative; or
□□using data for new purposes.

A PIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies. It is a tool, which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. The need for a PIA should be identified at an early stage and should consider building this into their project management or other business processes.

A PIA in relation to Regional OH project, would be to minimise the risk of informational privacy – the risk of harm through use or misuse of personal information. Risks which could arises from using, storing and sharing personal
data are:
□□inaccurate, insufficient or out of date;
□□excessive or irrelevant;
□□kept for too long;
□□disclosed to those who the person it is about does not want to have it;
□□used in ways that are unacceptable to or unexpected by the person it is about; or
□□not kept securely.
Projects which might require a PIA
The core principles of PIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals. A PIA is suitable for a variety of situations:
□□A new IT system for storing and accessing personal data.
□□A data sharing initiative where two or more organisations seek to pool or link sets of
personal data.
□□A proposal to identify people in a particular group or demographic and initiate a course of
action.
□□Using existing data for a new and unexpected or more intrusive purpose.

□□A new surveillance system (especially one which monitors members of the public) or the
application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
□□A new database which consolidates information held by separate parts of an organisation.
□□Legislation, policy or strategies which will impact on privacy through the collection of use
of information, or through surveillance or other monitoring.

Responsibility for conducting a PIA
A Data Protection Officer (DPO) is best placed to co-ordinate and carry out a PIA. Where there isn't a DPO, it can be done by project and/or risk managers, in consultation with other staff in the organisation, who will each be able to identify different privacy risks and solutions.
A PIA is linked to all the Data Protection 8 principles. Other topics covered in the Code of Practice are: Integrating PIAs with project and risk management; Mapping project and risk management concepts onto the PIA process; and Key methodologies and PIAs.
Overview of the PIA process

1. Identifying the need for a PIA.
The need for a PIA can be identified as part of an organisation's usual project management process or by using the screening questions in Annex One of the Code.

2. Describing the information flows.
Describe the information flows of the project.
Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information.

3. Identifying the privacy and related risks.
Some will be risks to individuals, eg, damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy.
Some risks will be to the organisation, eg, damage to reputation, or the financial costs or a data breach.

Legal compliance risks include the DPA, PECR, and the Human Rights Act.

4. Identifying and evaluating privacy solutions.
Explain how you could address each risk.
Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.
Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.

5. Signing off and recording the PIA outcomes.
Make sure the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.
A PIA report should summarise the process, and the steps taken to reduce

the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.
Publishing a PIA report will improve transparency and accountability, and let's individuals learn more about how your project affects them.

6. Integrating the PIA outcomes back into the project plan.
The PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.
A PIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored.
Record what you can learn from the PIA for future projects.
These steps are fully explained below. The template in Annex Two can be adapted to produce something which allows the organisation to conduct effective PIAs integrated with your project management processes.

Annex One

Privacy Impact Assessment Screening Questions
These questions are intended to help organisations decide whether a PIA is necessary.
Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.
You can adapt these questions to develop a screening method which fits more closely with the types of project you are likely to assess.

Screening Questions
Will the project involve the collection of new information about individuals?
Will the project compel individuals to provide information about themselves?
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
Will the project require you to contact individuals in ways which they may find intrusive?

Annex Two
Privacy impact assessment template

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example, a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows
The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements
Explain what practical steps you will take to ensure you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PIA process.

Step three: identify the privacy and related risks
Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register. Annex three can be used to help identify the DPA related compliance risks.
Privacy issue
Risk to individuals
Compliance risk
Associated organisation / corporate risk

Step four: Identify privacy solutions
Describe the actions you could take to reduce the risks, and any future steps which would be necessary, (eg, the production of new guidance or future security testing for systems).
Risk
Solution(s)
Result: is the risk eliminated, reduced, or accepted?

Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes
Who has approved the privacy risks involved in the project? What solutions need to be implemented?
Risk Approved solution Approved by

Step six: Integrate the PIA outcomes back into the project plan
Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork?
Who is responsible for implementing the solutions that have been approved?
Who is the contact for any privacy concerns which may arise in the future?
Action to be taken
Date for completion of actions
Responsibility for action

Contact point for future privacy concerns