Home Office

National ANPR Standards for Policing

Part 3 – Data Access and Management Standards

Version 2.0
October 2014

Change History

Version No.	Date	Details of Changes included in Update	Author
1.1	12.12.13	First Draft	Bill Mandeville
1.2	03.01.14	Revision to Appendix B	Bill Mandeville
1.3	06.01.14	Minor revisions	Bill Mandeville
1.4	12.02.14	Minor revisions	Bill Mandeville
1.5	24.03.14	Updated Glossary and revision of authorised LEA and other revisions.	Bill Mandeville
1.6	25.03.14	Revised table for data access	Bill Mandeville
1.7	25.03.14	Minor revisions	Bill Mandeville
1.8	09.04.14	Revised table for data access	Bill Mandeville
1.9	09.05.14	Minor revisions	Bill Mandeville
1.10	17.06.14	Additional access provision re Code of Ethics	Bill Mandeville
1.11	08.07.14	Revisions re data access	Bill Mandeville
1.12	18.07.14	Updated following Security &Data Management Special Interest Group meeting	Bill Mandeville
1.13	24.07.14	Updated following M Jones Review	Bill Mandeville
1.14	18.09.14	Revised following MPS and ICO liaison and Investigator and Analyst SIG input	Bill Mandeville
1.15	29.09.14	Revised re change from MOPI to APP	Bill Mandeville
2.0	15.10.14	Version 2.o as approved by the ANPR National User Group	Bill Mandeville

CONTENTS

1 Introduction

1.1 In order to facilitate the development and integration of Automatic Number Plate Recognition (ANPR) systems used by law enforcement agencies (LEAs), a set of standards have been developed by the National ANPR Programme Team on behalf of the Association of Chief Police Officers of England, Wales and Northern Ireland (ACPO), Police Scotland and other LEAs who connect to or have access to the National ANPR Infrastructure (NAI). These are the National ANPR Standards for Policing (NASP). The standards are consistent with the requirements of the Surveillance Camera Code of Practice issued under provisions of the Protection of Freedoms Act 2012 (PFA).

It is expected that these standards be adopted by LEAs throughout the UK.

1.2 NASP is divided into three parts:

Part 1 – Data Standards

Part 2 – Infrastructure Standards

Part 3 – Data Access and Management Standards

Part 1 (published separately) prescribes the standards with which data must comply in order for it to be accepted into the law enforcement NAI.

Part 2 (published separately) prescribes the standards for the components of the NAI including the operability standards required of back office systems that are to be used by LEAs and connected to the NAI.

Part 3 (this document) prescribes the standards required for access to and management of ANPR data within the NAI.

1.3 This document supersedes any previously published versions.

2 Applicability

2.1 These standards apply to any ANPR systems operated by police forces and other LEAs, throughout the UK, that connect to, or have access to, the NAI. ANPR systems include the Number Plate Reading Device (NRD), the Back Office Facility (BOF), communications links, firewalls and other related supporting components, including those components that are under the ownership or control of other organisations.

2.2 An organisation may only connect to, or receive data from, the NAI following approval of the Policing Lead for ANPR through the National ANPR Programme (an “Approved LEA”). Reference to LEA within all parts of NASP is in respect of ‘Approved LEA’ unless indicated otherwise.

2.3 The Policing Lead for ANPR will maintain a list of LEA. (Current list at Appendix A)

3 Legal Basis

3.1 ANPR data is police information within the meaning of The Code of Practice on the Management of Police Information 2005 (MoPI) made under the Police Act 1996 and Police Act 1997 and may be shared between LEAs in accordance with the provisions of that Code or any other document which applies similar standards in its place including the National Crime Agency’s (NCA) Statement of Information Management Practice (SIMP).

3.2 Access to and the retention and management of ANPR data obtained by LEAs must be compatible and consistent with obligations that arise under:

i. The Data Protection Act 1998 (DPA) and, as and to the extent to which they apply, with the data protection principles contained within Part 1 of Schedule 1 to the Act;

ii. The Human Rights Act 1998, and in particular Article 8 of the European Convention on Human Rights, namely the right to respect for family and private life;

iii. The Surveillance Camera Code of Practice issued under provisions of the Protection of Freedoms Act 2012 (PFA);

iv. "In the Picture" – Information Commissioner;

v. Criminal Procedure and Investigations Act 1996;

vi. College of Policing Approved Professional Practice – Information Management.

4 Data Controller

4.1 The data controller is the chief officer for the LEA that owns or controls the NRD that initially captures the 'read' data and stores it within a BOF that submits data to the NADC, or in respect of a list of vehicles of Interest (VOI), that creates that list. The chief officers of LEAs contributing data to the National ANPR Data Centre (NADC) are "data controllers in common" with respect to that data. A person may be authorised to undertake the responsibilities arising from these standards on their behalf.

4.2 Authorised members of LEAs may access and use data within the NAI without reference to the data controller unless otherwise required within the terms of NASP.

4.3 It is recognised that an LEA may receive data from ANPR systems not directly within its control in circumstances where it is using shared collection equipment that is owned and managed by a non-LEA organisation. In these circumstances, the chief officer of the LEA and the organisation owning the collection equipment are both data controllers who will store data in separate databases that they manage independently. The chief officer for the LEA is a data controller for data received under any such arrangement and as data controller may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment.

4.4 The LEA data controller must ensure that a formal agreement is in place, with the owner of the NRD and other components of the ANPR infrastructure that details appropriate arrangements to enable their compliance with NASP.

4.5 Where an LEA grants access to data from a NRD within its ANPR environment to another LEA, such that the data is submitted directly to, and stored within, a BOF outside of its ANPR environment, at or shortly after the time of initial capture, the ANPR chief officer lead for the LEA that owns the BOF that receives the data is data controller for the data that they receive. In managing that data they must take account of any conditions applicable to the grant of that access.

4.6 The technical capabilities of ANPR BOF enable the exchange of data between BOFs, the submission of data to the NADC and to access data held on the NADC. These standards make provision for an LEA to access ANPR data held by another LEA, or by the Home Office on their behalf, within the terms of NASP, and without a requirement for specific authority to be provided by the data controller for each occasion that access is required.

4.7 Where an LEA access data held by another LEA they are Data Controller for any data received as a result of that access. Management of data that is received must be in accordance with the provisions within NASP.

5 Access to ANPR Data

5.1 Policy

5.1.1 All LEAs that connect to, or have access to, the NAI must have a written policy in place in respect of the access, management and use of ANPR data, including provisions for audit.

5.2 Provisions for Data access

5.2.1 Access to data must be solely for law enforcement and investigation purposes as defined in Appendix B

5.2.2 Access to data will only be by personnel that have been granted access to the extent relevant to their role, in accordance with policy in an LEA which is consistent with the purposes and standards within this document, and specific requirements as shown within the table at Appendix C;

5.2.3 Where an authorisation for access is required, staff that may provide that authorisation must ensure that access is proportionate in each case taking account of the DPA and associated principles and that access is in the interest of justice.

5.2.4 Each LEA will designate a member of staff of at least superintendent rank, or equivalent staff grade in non-police LEAs, who is accountable for the authorisation of staff who may access ANPR data.

5.2.5 Personnel will only be granted access to ANPR data to an extent that is necessary and proportionate to their role. LEAs must ensure that authorised staffs are fully aware of the provisions within NASP.

5.2.6 LEAs will maintain a list of authorised staff and ensure that a persons' authorisation is revised or cancelled as appropriate when they change role.

5.2.7 The management of any data obtained must be consistent with the requirements of NASP.

5.2.8 Where ANPR data obtained is retained as material within the meaning of the Criminal Procedure and Investigations Act 1996 (CPIA) (or similar procedures in Scotland), the data controller[1] with responsibility for the NRD that recorded that data will be consulted before preparation of disclosure schedules and before data is used as evidence in court proceedings.

5.2.9 Subject to any legal obligation which imposes a contrary requirement, or circumstances in 5.2.11 below, information obtained from ANPR systems owned by other LEAs, or from the NADC, is not to be disclosed to any third party, including staff from an LEA that is not an 'Approved LEA', or the data subject, except through or with the express written authority of the data controller[2] with responsibility for the NRD that recorded that data, In all cases, the data controller will be contacted prior to information being disclosed.

---

[1] The data controller may authorise staff within the LEA to deal with disclosure of information and data relating to the ANPR system on their behalf.

[2] As 1 ante

5.2.10 Where an LEA has an active role in collaboration with another LEA which is not itself an 'Approved LEA' in the conduct of an investigation, the results of a search of ANPR data may be disclosed to that other LEA with a requirement that it is not further disclosed without the express written authority of the data controller.[3]

5.2.11 In addition to 5.2.9 and 5.2.10 above, any information regarding the location of NRD and other ANPR assets will not be disclosed without the written consent of the data controller[4] with responsibility for the NRD that recorded that data or, in the case of any legal requirements to disclose such information, before the data controller is provided with a specific opportunity to make representation to any court that is to consider an order for information to be disclosed.

6 Record Retention and Deletion

6.1 Capture records must be deleted no later than two years after their initial capture, unless retained under provisions of the Criminal Procedure and Investigations Act (CPIA) 1996 or similar provisions in Scotland.

6.2 Records that are identified as incorrect for any reason must either be corrected or deleted at the time that they are found to be inaccurate.

7 Records of Data Access

7.1 LEAs are required to maintain a record of any access by their staff to ANPR data, including details of the reason for access and a record of any authorisation for that access in a readily retrievable form.

7.2 LEAs are required to maintain a record of any escalation of an investigation to the category 'Major Investigation' or 'Serious Investigation', including details of the reason for escalation, in a readily retrievable form.

7.3 Records for data access and any change of investigation category will be made available to the Information Commissioner, the Surveillance Camera Commissioner and the Home Office on request for audit and monitoring purposes.

8 Audit of Access to ANPR Databases

8.1 LEAs accessing data held within another LEA ANPR environment are data processors on behalf of the data controllers for that data. LEAs will support all data controllers in the monitoring and audit of access to ANPR systems.

8.2 The Home Office is the data processor on behalf of the data controllers for all data that is held on the NADC. LEAs will support the Home Office in the monitoring and audit of access to the NADC and will provide relevant information on request.

8.3 Staff conducting activity in respect of monitoring and audit of the NADC on behalf of the data processor will have a current security clearance to SC level and national police vetting Level 3.

---

[3] As 1 ante

[4] As 1 ante

8.4 LEAs will audit the access to ANPR data obtained from other LEAs and by access to the NADC by their staff and maintain a record of all audits that are undertaken. Details of such audits will be made available to the relevant data controller for that data, Information Commissioner, the Surveillance Camera Commissioner and the Home Office on request.

9 Further Details

Any enquires in relation to NASP should be addressed in the first instance to the National ANPR Programme Team at anpr@homeoffice.gsi.gov.uk.

Glossary of Terms, Abbreviations and Definitions

ABH	Actual Bodily Harm
ACPO	Association of Chief Police Officers
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers and Back Office Facility
BOF	Back Office Facility
Capture	The process by which a VRM is read
CPIA	Criminal Procedure and Investigations Act 1996
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement and compliance activities
MOPI	Management of Police Information
NASP	National ANPR Standards for Policing
NADC	National ANPR Data Centre
NAI	National ANPR Infrastructure
NCA	National Crime Agency
NIM	National Intelligence Model – A structured intelligence business process within LEA
NRD	Number Plate Reading Device
PFA	Protection of Freedoms Act 2012
SIMP	Statement of Information Management Practice – applies to NCA
SIO	Senior Investigating Officer
TIC	Taken into Consideration – A procedure to enable offences to be dealt with by a court without each to be formally prosecuted
VOI	Vehicle of Interest (a list of VOI was previously referred to as a ‘hot list’)
VRM	Vehicle Registration Mark

APPENDIX A
Approved LEAs

ACPO Vehicle Crime Intelligence Service (AVCIS)
Avon and Somerset Constabulary
Bedfordshire Police
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Civil Nuclear Constabulary
Cleveland Police
Cumbria Constabulary
Derbyshire Constabulary
Devon and Cornwall Constabulary
Dorset Police
Driver and Vehicle Standards Agency (DVSA)
Durham Constabulary
Dyfed-Powys Police
Essex Police
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
H M Revenue & Customs (HMRC)
Humberside Police
Kent Police
Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Merseyside Police
Metropolitan Police Service
Ministry of Defence Police
National Crime Agency (NCA)
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
Police Scotland
Police Service of Northern Ireland (PSNI)
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police
Thames Valley Police
Warwickshire Police
West Mercia Constabulary
West Midlands Police
West Yorkshire Police

APPENDIX B

Investigation Categories

Investigations within LEAs fall within three main categories, so that there is a consistency of understanding within LEAs as to which investigations should be included within each category. The main categories are:

- Major Investigations
- Serious Investigations
- Priority and Volume Investigations

A consideration of the category of the investigation informs effective management and decision making, including the scope for an investigation and determination of the resources that are to be deployed. These categories provide the framework to support a National policy for retention of, and access to ANPR data. The categorisation of an investigation should be determined taking account of the circumstances in each case, using the below framework as a guide.

Major Investigations

A key characteristic is that Major Investigations should be normally be led by a Nationally Registered Senior Investigating Officer (SIO) within a police force or similarly senior investigator in non-police LEAs.

Designated Major Investigations

Murder
Attempted Murder
Manslaughter
Infanticide
Child Destruction
Kidnapping
Terrorist related crimes

Designated Serious Investigations

Arson
Abduction
Aggravated Burglary dwelling and non dwelling
Arson High Value or life endangered
Blackmail
Drug Trafficking
Death by Dangerous Driving
Female Genital Mutilation
Fraud and Associated Offences (80hrs + investigation time)

Gross Indecency Child
Perverting Justice
Public order (racially motivated)
Rape
Robbery (Firearms or ABH or more serious injury caused)
Sexual Assault (children under 13)
Threats to Kill
Vulnerable Missing Person
Wounding (S18/20)
Response to incidents of significant public interest / public safety

Serious Investigations may, with the authority of a Superintendent, or equivalent staff grade in non-police LEAs, be escalated to the category of Major Investigations.

Investigations that have been escalated to serious from the category of Priority and Volume Investigations may not be further escalated to the category of major Investigation.

Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded. Any authority to escalate will take account of the following factors:

Escalation Factors

Consideration	Examples
Community factors	• Likely to escalate into large scale disorder or critical incident • Has escalated from a previous offence • Sensitivity regarding individuals involved
Offence characteristics	• Aggravating factors of the offence • Vulnerability of victims/witnesses, • Has crossed force or national boundaries • Forms a previously undetected series
Offender Characteristics	• Organised crime • Terrorism links • Resistance to police operational strategies • Multiple offenders

Priority and Volume Investigations

Investigations not included within the above categories will be considered as within the remit of Priority and Volume Investigations. In particular, this will include investigations into street robbery, burglary and vehicle-related criminality and non-crime issues such as anti-social behaviour, vehicle excise offences and road traffic offences and missing persons.

Priority and Volume Investigations may with the authority of an Inspector, or equivalent staff grade in non-police LEAs, be escalated to the category of Serious Investigations.
Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded and will take account of the following factors:

Escalation Factors

Consideration	Examples
Community	• High risk of critical incident • Sensitivity regarding individuals involved

Offence Characteristics	• Aggravating factors of the offence such as:
	  • Hate crime
	  • Weapons used
	  • Injuries sustained
	  • Vulnerability of victims/witnesses,
	• Priority issue identified within NIM business process.
	• Series of offences e.g. forensic links to the offender(s)
	• Complexity of the Investigation

Offender Characteristics	• Criminal history • Resistance to investigative strategies • Prolific offender • Multiple offenders

APPENDIX C
Data Access Requirements

Age of data to be accessed (as required)	Purpose of access to data
	To monitor alarms or receive reports from matches against a list of Vehicles of Interest (VOI) from a NRD for operational response or intelligence purposes
Real or near real time during the course of monitoring	By any member of staff authorised to access ANPR systems with no additional authority required.
	To research data for 'Priority and Volume Investigation' purposes (Appendix B)
Up to 90 days	By any member of staff in accordance with their authorisation to access ANPR systems.
Over 90 days	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of an Inspector or equivalent staff grade; a) where there has been a significant delay in reporting the offence to be investigated, or; b) new information or evidence has become available, or; c) the investigation is being conducted diligently and expeditiously and is not yet completed.
	To research data for 'Serious Investigation' purposes (Appendix B)
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.
Over 1 year	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of an inspector or equivalent staff grade; a) where there has been a significant delay in reporting the offence to be investigated, or; b) new information or evidence has become available, or; c) the investigation is being conducted diligently and expeditiously and is not yet completed.

	To research data for 'Counter Terrorism' or other 'Major Investigation' purposes (Appendix B)
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.
Over 1 year	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of an inspector or equivalent staff grade.
	To prepare evidential material for information revealed during a previous search of ANPR data.
	By any member of staff in accordance with their authorisation to access ANPR systems with no additional authority required.
	To comply with a written request from the Crown Prosecution Service, the procurator fiscal or on the direction of a court.
	By any member of staff in accordance with their authorisation to access ANPR systems with no additional authority required.
	To research data as part of an investigation into alleged breach of the policing Code of Ethics
	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of a superintendent or equivalent staff grade.