Home Office

National ANPR Standards for Policing and Law Enforcement

November 2020

Version: 2.1

1. Executive Summary

These standards articulate the requirements with which the police and other Law Enforcement Agencies (LEA), as detailed at Annex A must comply to access the National ANPR Capability (NAC). These standards do not cover the use of Automatic Number Plate Recognition (ANPR) for any purpose that is not law enforcement and will identify the purposes for which this document shall be applicable. Data from the NAC may not be used for other purposes, however in appropriate circumstances a camera may provide data to both the NAC and organisations other than those listed at Annex A to be managed independently.

This document includes a description of the legal basis for ANPR as well as the applicability of these standards. The standards comprise three main sections: Data Standards, Infrastructure Standards and Data Access and Management Standards. Audit standards and technical requirements are covered in other documents.

Data Standards comprise the security requirements that must be met for the NAC as well as the composition requirements for read data.

Infrastructure Standards cover the end-to-end infrastructure requirements for the NAC, including infrastructure development, cameras, networks, databases, infrastructure access and performance and legal requirements.

Data Access and Management Standards include the management of data within the NAC, including collection, storage, transfer and deletion of data. This section also provides guidance on FOI and Data Protection Act (DPA) enquiries.

The Annexes to this document include password requirements, guidance on investigation categories, the approval process for accessing ANPR data and a list of approved organisations that may access ANPR.

2. Contents

Document Revisions

Version 1.1 draft	July 2020	Change ref from CAST to DSTL in 8.14 Clarification at 9.8 re Command and Control Update of links within text
Version 2.0	September 2020	Published with amendments as above
Version 2.1	November 2020	Footnote added re data deletion (para 9.5.1)

Definitions

Acronym	Description
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
Audit Standards	National Standards for Compliance and Audit of Law Enforcement ANPR
CCTV	Closed Circuit Television
CAMERA	The device used to capture an ANPR read
CAPTURE RECORD	The record of a vehicle recorded by NAS for a vehicle passing an ANPR camera including the ANPR READ, associated images and meta data.
COMMUNICATIONS LINKS	The connections between the camera, any local infrastructure and the NAS
CONTROLLER	The competent authority which alone or jointly with others determines the means and purposes of the processing of personal data. Part 3 data Protection Act 2018
CCA	Crime and Courts Act 2013
CPIA	Criminal Procedure and Investigations Act 1996 and the CPIA Code of Practice
DPA	Data Protection Act 2018
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
GSCP	Government Security Classifications Policy – (formerly the Government Protective Marking Scheme (GPMS)
GPS	Global Positioning System
HIT	The report of a match of a vehicle registration mark (VRM) READ with a VRM that is included on a vehicle of interest list (VOI)
ICO Code	ICO Code of Practice for Surveillance Camera Systems

ISO	Information Security Officer – The member of staff with responsibility for ensuring compliance with requirements for IT security
ITHC	IT Health Check – The process for ensuring that security provisions for IT are appropriate and in compliance with requirements that are current at the time of the check.
JCA	Joint Controller Arrangements under provisions of the Data Protection Act 2018-
JPEG	Joint Photographic Expert Group image format
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities. For the purpose of this document, LEAs shall only include those organisations listed at Annex A.
MIDAS	Motor Insurance Bureau (MIB) data of uninsured vehicles
MOPI	Code of Practice for the Management of Police Information
NAC	National ANPR Capability includes: • the NAS which is a single national system consisting of the functionality to enable use for operational response, investigation and intelligence purposes and a single national store of data, and, • the National ANPR Infrastructure (NAI) which is a network of ANPR cameras, communications links, firewalls and other related supporting components, that are the responsibility of LEA, that connect to the NAS.
NAI	A network of ANPR cameras, communications links, firewalls and other related supporting components
NAS	National ANPR Service
NASP	National ANPR Standards for Policing first version published in 2013 and replaced by NASPLE recognising the applicability to all law enforcement agencies that access the NAS
NASPLE	National ANPR Standards for Policing and Law Enforcement.
National VOI List	Nationally circulated lists that include stolen vehicles, vehicles requiring an operational response and vehicles within Schengen circulations
NAPS	National Accreditor for Police Systems – Responsible for confirming that police IT systems are in accordance with security requirements and authorising connection to national systems.
Network Connections	The IT links between components of the NAC

NPCC	National Police Chiefs' Council
NPCC Vetting Policy	The NPCC standards for vetting of staff for access to police information
PERSONAL DATA	Means any information relating to an identified or identifiable living individual. 'identifiable living individual' means a living individual who can be identified directly or indirectly, in particular by reference to_ a) an identifier such as name, an identification number, location data or an online identifier, or b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual Data Protection Act 2018
PNC	Police National Computer
READ	The interpretation of a VRM by an ANPR system
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
SMS	A Standards format for text messaging
TSpec	The document prescribing the technical specifications for data within the National ANPR Service (NAS) to comply with the requirements of NASPLE.
VOI	The details of a vehicle that are of interest to law enforcement for operational response or investigation purposes that is included on a list to enable it to be READ and for authorised staff to receive a report of that READ.
VRM	Vehicle Registration Mark

3. Introduction

The Home Office issues these standards in support of the management and use of the National ANPR Service (NAS). ANPR is used by the police and other law enforcement agencies (hereafter referred to as LEAs) for law enforcement purposes. LEAs should use these policy standards to shape technical standards, standard operating procedures and audit standards.

This document covers the use of ANPR within the NAC and will identify for which uses this document shall be applicable. The use of ANPR within the NAC otherwise than in accordance with this document is not permitted.

This document is divided into 3 sections:

- Part 1 – Data Standards, which define the compliance requirements for ANPR Data
- Part 2 – Infrastructure Standards, which define the compliance requirements for ANPR infrastructure
- Part 3 – Data Access and Management Standards, which define the access requirements for LEAs and other organisations that are associated with ANPR data for law enforcement purposes.

4. Background

ANPR technology is used to help detect, deter and disrupt criminality at a local, force, regional and national level. This includes tackling traveling criminals, Organised Crime Groups and terrorists. ANPR provides lines of enquiry and evidence in the investigation of crime and is used by LEAs throughout England, Wales, Scotland and Northern Ireland.

There exists a National Law Enforcement ANPR capability (NAC) which enables LEAs to benefit from operational use of ANPR. The NAC comprises:

- The NAS. This is a single national system comprising standardised functionality to enable use for operational response, investigation and intelligence purposes as well as a single national store of data;
- The National ANPR Infrastructure (NAI), which is a network of ANPR cameras, communications links, firewalls and other related supporting components. Any element of this network that is connected to the NAS shall be the responsibility of the LEA that manages that connection.

4.1 Technical Specifications

Technical specifications for the NAC are detailed within a technical specification document (TSpec). LEAs are required to conform to the requirements of that document.

5. ANPR Legislation

ANPR operates under a complex framework of legislation of general application, including the General Data Protection Regulation (GDPR), the DPA, the Surveillance Camera Code and Common Law.

The National Law Enforcement ANPR capability (NAC) is subject to the Information Commissioner's Office regulatory provisions and regulatory oversight by the Surveillance Camera Commissioner (SCC).[1]

5.1. ANPR Data: Legal Basis

ANPR data from police forces 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. It 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).

Access to and the retention and management of ANPR data obtained by LEAs must be compatible and consistent with their relevant legal obligations, which include: The Data Protection Legislation (i.e. the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA));

- ICO Code of Practice for Surveillance Camera Systems (ICO Code);
- College of Policing Approved Professional Practice – Information Management. (MOPI);
- Part 2 of the Protection of Freedoms Act 2012 (PoFA);
- The Surveillance Camera Code issued under Part 2 of PoFA.
- Criminal Procedure and Investigations Act 1996 and Code of Practice issued under Part II of that Act (CPIA);

[1] Section 29(6) of the PoFA includes ANPR as one of a number of surveillance camera systems under the regulatory oversight of the SCC and its associated Home Office code of practice. Relevant authorities (as defined by Section 33 (s33) of PoFA) in England and Wales (including the police) must have regard to the code which provides guidance on the appropriate and effective use of surveillance camera systems, and therefore ANPR

5.2. Use of ANPR for Law Enforcement Purposes

ANPR infrastructure may only be deployed law enforcement purposes as defined in Part 3 of the DPA ; or on grounds of national security. Law Enforcement is defined by the DPA as “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”. The Joint Controller Arrangements (JCA).

The JCA details the responsibilities of controllers for compliance with the DPA. The National Police Chiefs’ Council (NPCC) ANPR lead is designated as the lead controller within the JCA for the NAS.

Joint Controllers have determined within the JCA that they will conform to consistent policy and procedures for the elements of the NAC for which their own LEA is responsible and for which they are controller.

5.3. ANPR Audit

The Home Office has also issued a separate document entitled “National Standards for Compliance and Audit of Law Enforcement ANPR” (Audit Standards). This document sets out the requirements for compliance and audit by all LEAs and of the national components of the NAC.

6. Applicability

These standards apply to any NAC operated by LEAs in the UK that connect to or receive data from the NAS.

Where, under an agreement, LEAs receive data from components that are under the ownership or control of other organisations it is the responsibility of the receiving LEA to ensure compliance with the NASPLE.

ANPR cameras that are used solely for speed enforcement are outside the scope of these standards.

ANPR systems that are not operated by LEAs and do not submit data to the NAS are similarly outside the scope of these standards.

6.1. Approved Organisations

An LEA may only connect to, or receive data from, the NAS following approval of the NPCC policing lead for ANPR within the NPCC Crime Operations Committee (NPCC policing lead for ANPR) - an "Approved Organisation".

For an organisation to be designated as an "Approved Organisation" it must be involved in and can lawfully process data for one or more of the following activities:

- National security and counter terrorism
- Law enforcement
    - The prevention and detection of crime
    - The apprehension and prosecution of offenders

In granting access, the NPCC policing lead for ANPR must be satisfied that it is necessary and proportionate for the organisation to be approved.

Approved Organisations must ensure that their organisation complies with the requirements of NASPLE and Compliance and Audit Standards.

References to LEAs within NASPLE includes only "Approved Organisations" unless indicated otherwise. Approved Organisations are listed in Annex A.

In addition to the above purposes LEAs may use the NAS for operational purposes relevant to individual and public safety. E.g Missing persons.

7. Part 1: Data Standards

7.1. Data Standards Overview

Part 1 prescribes the standards with which data must comply for it to be accepted into the NAS.

7.2. Data Security

LEAs have a duty to protect ANPR data to ensure its integrity and to maintain its value for law enforcement purposes. ANPR 'read' data must therefore be attributed a protective marking of OFFICIAL, in accordance with the Government Security Classifications Policy (GSCP).

When in the NAS database, other material could be accessed such that personal details of persons associated with the ANPR READ data may be identified. Once ANPR READ data is available within the NAS, it is personal data in the context of the DPA.

All ANPR data in the NAS, should therefore be managed in accordance with DPA principles and handled as OFFICIAL - SENSITIVE data, in accordance with the GSCP.

Whilst in the custody of, or being transmitted to or from a LEA, ANPR data should be handled in accordance with Part 2 and Part 3 of NASPLE.

Access to data within ANPR systems must be in accordance with Part 3 of NASPLE.

7.3. ANPR Read Records

7.3.1. Composition

An ANPR READ places a VRM at a specific location and time. It is obtained by a camera as part of an automatic number plate reading system. The data components of a record must not be entered manually into the NAS unless for the purposes of correcting a mis-read VRM on the system or by an administrator for testing the connectivity of a camera.

The READs must include VRM, time, location of read and camera identifier and be consistent with the requirements of section 7.4.

7.4. Core Data

7.4.1. Vehicle Registration Mark (Mandatory)

ANPR data must accurately represent VRMs of all vehicles with correctly represented EU and Schengen Community number plates. Systems must accurately record the VRM for vehicles passing within the field of view for each camera. The capture and read rates must be in accordance with the type of camera defined at Section 8.9.

7.4.2. Vehicle Registration Mark – Not Read (Mandatory where functionality is in place)

Where a CAMERA has the capability to record images of vehicles passing within the field of view where no VRM is identified by the system, information will be recorded in the VRM field in accordance with current TSpec.

7.4.3. Time (Mandatory)

System audit provisions must provide evidence of synchronisation at least once every 10 minutes using standard time source techniques in accordance with current TSpec.

Components of ANPR systems must automatically adjust the display of the time to daylight saving time during the period when this is in-force.

7.4.4. Location (Mandatory)

ANPR data must place a read in a location, accurate to within 10 metres. In addition, all fixed-site ANPR cameras must have their GPS co-ordinates accurately recorded to within 5 metres.

7.4.5. Supporting Imagery

In order to assist with assessment of the accuracy of individual read records, ANPR data may include images:

- Plate patch – showing the number plate only, to allow comparison of the visual image with the textual representation interpreted (Mandatory for systems under ownership or control of a LEA)

- Overview Image – showing the vehicle to allow identification of the make, model and colour of the vehicle within the read zone (Optional)

- ‘Geo Tagging’ - if an accurate GPS Geo Location is available, then this detail may be added to images (Optional)

Should any image be found to exceed prescribed limits for image size, cameras submitting the images must be revised to ensure images obtained are within the limits prescribed within a maximum of 7 days.

All images must be linked to the corresponding read record.

All images recorded must be forwarded to the NAS. Where no overview image has been recorded, the read record must include a reference to identify that no image is recorded.

7.4.6. Record Retention and Deletion

All read records received by LEAs including any associated images must be supplied to the NAS.

All records must be managed and subsequently deleted in accordance Section 9.5.

7.4.7. Camera Performance Evaluation

Camera Performance evaluation, as detailed in Section 8.14 of all components within LEA ANPR systems must be conducted to ensure compliance with the Data Standards. Where performance falls below the Data Standards then this must be corrected and reassessed to confirm that performance conforms to data standards, within 30 days of that issue being identified.

If camera performance issues are not resolved within 30 days of identification, then the feed of data from those cameras must cease until corrected.

8. Part 2: Infrastructure Standards

8.1. Infrastructure Standards Overview

Part 2 prescribes the standards for the components of the NAC, including the operability standards required that are to be used by LEAs connected to the NAS.

8.2. Accreditation

To preserve the integrity of the NAC, all components of infrastructure that connect to the NAS must be assessed to ensure that they do not pose a threat to the NAC and are suitably for handling data up to GSC OFFICIAL level.

8.3. LEA Domain

The assessment of risk to an LEA domain rests with the controller for each LEA, which will normally be discharged by the Information Security Officer (ISO) for that LEA. The level of risk posed should be determined through completion of a Risk Analysis Document and an IT health check (ITHC). Review of compliance with the risk analysis outcomes and the conduct of an ITHC is to be completed annually.

8.4. ANPR Network

The National Accreditor for Police Systems (NAPS) needs to be assured that the local LEA Infrastructure poses no threat to NAC. The NAPS will liaise with the LEA ISO to assess the level of risk posed, as documented through the LEA corporate information risk management and ITHC process.

The NAPS will approve the components of local infrastructure for connection to the ANPR Network. This will be confirmed by the completion of the Code of Connection.

8.5. ANPR Infrastructure Development

A consistent and standardised approach must be applied to infrastructure development within the NAC.

8.5.1. Strategic Assessments

A strategic assessment should be carried out prior to the deployment of an ANPR camera. An assessment should also be carried out prior to receiving ANPR data for onward submission to the NAS, that is received from ANPR systems operated by organisations that are not defined as LEAs. These assessments must identify a need for ANPR at that location for law enforcement purposes.

Where a need is identified, consideration of whether the deployment, or the receipt of ANPR data is appropriate and proportionate. This requires an assessment of the value for law enforcement purposes taking account of the impact on fundamental rights and freedoms of individuals. Consideration of the legitimate expectations of individual privacy is also required. Strategic assessment should consider:

- National Security and Counter Terrorism,
- Serious, Organised and Major Crime
- Local Crime,
- Community Confidence and Reassurance, Crime Prevention and Reduction.

8.5.2. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA), which may include consultations with relevant stakeholders, is required for all planned new infrastructure.

The DPIA must include:

- A description of the proposed development
- An assessment of the risks to the fundamental rights and freedoms of individuals – the data subjects.
- Measures to mitigate those risks
- Confirmation of safeguards and security measures to ensure protection of personal data and compliance with the DPA.
- Details of any stakeholder consultation

8.5.3. Information Commissioner's Office Consultation

The NAC may result in high risk to the rights and freedoms of individuals and prior consultation with the Information Commissioner's Office (ICO) may be required before the deployment of any new ANPR infrastructure. When a DPIA identifies a large increase in the number of deployed ANPR infrastructure or where significant privacy risks are identified the ICO should be consulted. (Section 64 DPA)

8.5.4. Strategic Assessment Reviews

LEAs must monitor the continued requirement for a camera to be maintained at a location, or for an LEA to receive data from ANPR systems operated by other organisations. Should the justification for deployment at that location cease, the device must be removed, and the receipt of data must be terminated.

The locations of all cameras and the need to receive data from systems operated by other organisations must be reviewed annually, considering requirements for infrastructure development to ensure that camera deployment or receipt of data remains appropriate and proportionate.

8.6. Vehicle-Mounted Systems

Vehicle-mounted ANPR may only be deployed where any of the following circumstances arise:

- For the purposes of monitoring hits against a list of VOI with the intention that an operational response to the hit will take place, either by staff within the vehicle containing the ANPR system or by others deployed in support of that vehicle for the purpose of providing a response.
- Deployed at locations identified following completion of infrastructure development assessment prior to the deployment of other camera at the location.
- Deployed as a result of Operational tasking processes within an LEA where it has been determined that it is proportionate for short-term deployment of ANPR;
  - In response to identified criminal activity
  - In response to identified community problems
- To support assessment of a location for future more permanent camera deployment in accordance with the infrastructure development procedure
- In support of immediate operational response following report of a crime or incident.

8.7. System Standards

The performance standards for camera shown below are most easily met for vehicles travelling towards a camera, and it is recommended that unless unavoidable, for example in some dual-lane deployments, that this configuration is used in all cases.

8.7.1. Static ANPR Systems

A static ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs and is located in a fixed position, with no intention of the system being moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye[2] and accurately read 95% of captured VRM.

8.7.2. Moveable ANPR Systems

A moveable ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs, is located in a fixed position on a temporary basis and may be

[2] 'Visible to the Human eye' should be determined from the viewpoint of the camera within the ANPR system. A number plate visible to a 'human eye' at that location should also be visible by the ANPR system.

moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.3. Multi-Lane ANPR Systems

A Multi-Lane ANPR system has the capability to read VRM for vehicles travelling in multiple lanes of the highway using a single camera. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. For vehicles travelling towards the camera, systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

For vehicles travelling away from the camera, the system must capture 90% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.4. CCTV Integrated ANPR Systems

A CCTV Integrated ANPR system may operate both as a CCTV camera and as an ANPR camera. The camera should be optimised[3] for the purposes of ANPR when being deployed as a camera. Integrated systems must only provide data to the NAS when in ANPR mode. Except in extreme weather conditions the performance standards for these systems must be achieved at all times when deployed in ANPR mode. CCTV systems may not be optimised to capture ANPR reads therefore systems must capture 85% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.5. Mobile ANPR Systems

A mobile ANPR system has been built for the primary purpose of ‘capturing’ and ‘reading’ VRMs. These include vehicle-mounted ANPR systems and other portable systems deployed on a temporary basis. Any equipment procured after the publication of version 1 of National ANPR Standards for Policing (NASP) (May 2013) must be live-linked to the NAS.

To achieve the optimum performance requirements, mobile equipment should be capable of night-time and low-light operation. Except in extreme weather conditions the performance standards for these systems must be achieved at all times.

Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM unless deployed in a moving vehicle, when the system must capture 80% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

[3] The optimum configuration of CCTV systems differs when used for general CCTV surveillance to when operated as an ANPR reader. It needs to be configured for ANPR use to ensure maximum possible data accuracy

8.7.6. Covert Systems

It is recognised that circumstances may arise where moveable or purpose-built, covert systems are deployed in support of an investigation in circumstances where it is not possible to establish a live-link to the NAS. Deployments of this type that are authorised within provisions of the RIPA or RIPSA are the only circumstances where equipment procured after the publication of version 1 of NASP (May 2013) may not have the capability to live-link to the NAS.

Unless unachievable due the nature of the deployment or in extreme weather conditions, the performance standards for these systems must be achieved at all times. Systems must capture 98% of al VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.8. Camera Access Settings

Unless a camera is designated a 'Restricted Access' camera, all cameras that submit data to NAS must be attributed the settings of 'Open Access', such that all data received from that camera is visible to all users with appropriate permissions to access the data.

With appropriate authority, a camera may be designated a 'Restricted Access' camera. Designation of a camera for 'Restricted Access' may only be authorised by a senior manager. A 'Restricted Access' camera may or may not be covert and the designation of a device for 'Restricted Access' may require authorisation within the provisions of the RIPA or RIPSA.

A record of all authorisations for restricted access must be retained for the duration of the restriction and a period of 2 years thereafter.

8.9. System Capability and Resilience

8.9.1. Image Capture

All cameras under the ownership or control of LEAs must have the capability to capture and record supporting imagery in accordance with section 7.4.5.

There may be circumstances where the shared collection equipment that is owned and managed by a non-LEA organisation is being used that are not enabled for the recording of imagery. In these circumstance, these cameras may be connected to the NAS subject to the standards for ANPR Infrastructure Development.

Supporting Images are important to assist with the accuracy of individual capture records and therefore, where data is received from other a non-LEA organisation without supporting images, provision for upgrading of the system to enable the provision of images should be established.

8.9.2. Schengen Information Systems (SIS)

All ANPR systems must be capable of reading plates that form part of the SCHENGEN community.

8.9.3. Data Storage

The NAS must not allow any data loss.

8.9.4. Local System Resilience

All local ANPR systems must transfer data to the NAS on receipt in local systems from a camera and also have the capacity to retain ANPR reads and their related images for a minimum of 3 and a maximum of 7 days from the time of the ANPR read.

This will provide resilience should the local infrastructure connections, the NAS or communications to the NAS become unavailable and will prevent the loss of data. In the event of a failure to send read records and associated images to the NAS local systems must have the capability to re-send that data.

If for any reason reads from a camera are submitted to the local system more than 7 days after initial capture the reads may be retained on the local system for 24 hours to prevent loss of data, should connection to the NAS become unavailable.

8.9.5. Local system connection and data transfer

Local ANPR systems must not enable connection to or the transfer of data to ANPR systems operated by other LEA for the purposes of searching of data or monitoring of VOI lists.

During the period of any loss of connection to NAS local functionality may provide for basic search of a full or partial VRM and for alerting against the most recent VOI lists received from NAS.

LEAs must not share VOI lists, even in circumstances of NAS unavailability; however, LEAs may share information and intelligence relating to those VOI lists using established intelligence management procedures.

8.9.6. Local system data deletion

Data held on local systems must be deleted within the next 24 hours after the period of 7 days following the time of the read. Where a read is submitted to the local components of NAC more than 7 days after the time of the read by a camera it may be retained for no more than 48 hours in local systems and then deleted within the subsequent 24 hours.

8.9.7. Extended unavailability of NAS

In the unlikely event that connections to the NAS are unavailable for more than 7 days, then deletion of data in accordance with the above provisions may be suspended until such time as connection is restored. This may only be done with specific authority of the controller for the LEA collecting the data and a full written record of the granting of that authority is required.

8.9.8. Mobile ANPR Systems Data Transfer

All ANPR data held on mobile ANPR units that have been unable to transmit their data in real time must be transferred to the NAS within a maximum period of 48 hours from the time of capture except in circumstances where the camera is unable to connect to the local system.

8.9.9. Support and Maintenance

ANPR systems should be commissioned only with an appropriate level of support and maintenance to safeguard against component failure and assist with business change. Local provisions must be in place to ensure that, in the event of any failure of a component of infrastructure that provides communications to the NAS, to prevent loss of data. Reinstatement must be within a period consistent with the ability to retain data locally for that failed component and subject to a maximum period of 72 hours from the time that the component failed.

8.10. System Connectivity

8.10.1. Local ANPR Infrastructure Connectivity to LEA networks

Local ANPR Infrastructure must connect to the LEA network infrastructure to allow user access to the NAS and to support connections to the Police National Computer (PNC) and the NAS.

The security of all infrastructure connections must be managed via an organisation maintained and managed firewall in accordance with that organisation's own policy and the Community Code of Connection and NPCC/Police Scotland Community Security Policy.

8.11. National Databases

NAS must have the capacity to check against the following national databases, as a minimum; PNC; Includes 'Fast Track' 'Extract', 'Schengen' and 'MMC' data.

8.11.1. Response Times

In order to ensure compliance with DPA principles in the circulation of VOI, Real-time matching performance standards must be achieved in 95% of all reads.

The following table summarises maximum response times within the NAC:

System Type	Read to alarm	Number plate read by a camera to delivery to NAS	NAS process to delivery at a LEA for visibility by staff
Static ANPR system	4 sec	2 sec	2 sec
Moveable ANPR system	4 sec	2 sec	2 sec
Multi-Lane ANPR System	4 sec	2 sec	2 sec
CCTV Integrated ANPR system	4 sec	2 sec	2 sec
Mobile ANPR system	6 sec	4 sec	2 sec

8.11.2. Real-Time Data Delivery

In order to ensure operational capability and to support compliance with DPA, local LEA ANPR infrastructure must clearly display the current state of connectivity to the NAS and/or any time when data is not being sent to the NAS. In the event of a communications or systems failure, the LEA infrastructure must buffer that read data and deliver it to the NAS once the communications or failed systems have been restored. The real-time delivery of data is a priority and the delivery of any buffered data should take place in addition to delivery of real-time data.

8.11.3. Search and Export of Data

The NAS must provide for the identification and export of data to enable identification using criteria defined in TSpec.:

The ability to export ANPR data shall be limited to defined users.

In appropriate circumstances a message may be sent to authorised users by means of SMS text. Where SMS is used the information provided will be limited to the VRM, time and location of the read and the name of the list containing the VOI.

Bulk data, including images, required for investigative purposes that is stored under provisions of the Criminal Procedure and Investigation Act 1996 (CPIA) may be exported to an external LEA defined storage area and managed in accordance with local policy.

The NAS must provide for user defined privileges for use of data export functions and data may only be exported by users with those privileges.

8.11.4. Security

The NAC must provide for adequate security measures, including access control, to protect against unauthorised access to the system and data held within it. LEAs must ensure compliance with NAC requirements and are accountable for the security of all components of the NAC that are within their control. LEAs must ensure that individual user privileges are consistent with the requirements of their role and individual level of vetting.

Audit trails must be maintained to record all significant actions taken, including:

- User login,
- Successful and failed database searches, and;
- the addition to, and deletion of data from lists of VOI.

There must be provision within the NAS for users to record the reasons and any required authorisation for their actions. Access to audit trails must also be auditable and restricted to users who require this access as part of their role, as defined within policy.

The security of all LEA components of the NAC must be managed via an LEA. The LEA shall maintain and manage a firewall in accordance with the LEA's own policy, the Community Code of Connection and Community Security Policy. The requirements of the national network connections and GSC as confirmed by the appropriate governance authority in each case.

8.12. Databases

8.12.1. National Database

LEAs that receive VOI lists and updates from a national VOI list shall ensure that this list is loaded on their mobile system at the first opportunity following receipt of that list or update.

8.12.2. Third Party Databases

Where data is provided by a third party (e.g. the MIDAS File as provided from the Motor Insurance database), then there must be measures/procedures to ensure that the data is handled consistent with these standards. The criteria that must be addressed through these procedures include:

- Provisions must be in place to ensure that only the most up-to-date data set is in use.
- Version control and file naming systems must be in place
- Distribution methods must be in accordance with GSC security requirements.

8.13. Lists of Vehicles of Interest

8.13.1. Vehicle of Interest List Purpose

Lists of Vehicles of Interest (VOI) may be maintained by LEAs to support intelligence development, operations and investigations. The contents of a list of VOI will depend upon the purpose of that list, the format for which is detailed in TSpec.

8.13.2. Vehicle of Interest List Information and Access Controls

VOI Lists used for monitoring purposes and that do not require an operational response may include the details defined within the Tspec. When a VOI List is used to support operational response, sufficient information to ensure an appropriate response must be included.

LEA may maintain a VOI list for operational response purposes; however, these lists should only be used in circumstances that do not meet the need to include the information on the PNC. Access permissions for those lists must be restricted to ensure that data access is proportionate in each case.

Special Categories of Data and Criminal Convictions Data as defined by Schedule 1 of the DPA and Articles 9.1 and 10 of GDPR should only be included within a VOI list when it is essential to the purpose of circulation. The LEA circulating the list must ensure that the content and provisions for the access to any such list are appropriate at all times.

8.13.3. Vehicle of Interest List Resilience

The NAS will make lists of VOI available to LEA in order that they can be loaded onto management servers and mobile systems should the live-link to NAS become unavailable.

LEAs must not load VOI lists received from NAS onto any other systems and must establish procedures to ensure that VOI lists loaded onto the management server or mobile systems are current versions of those lists.

8.13.4. Actions required for a Vehicle of Interest List

Any LEA publishing a list of VOI onto NAS will determine access controls for that list. Lists will only be accessible to LEAs where it is proportionate for that accessibility. Where one LEA subscribes to the VOI Lists of another LEA, there is an obligation to monitor the list, assess a ‘hit’ against the list and respond subject to local resource availability and operational demands.

Logs of the loading of any VOI list onto a mobile system shall be maintained as required by Section 9.10.

8.13.5. Vehicle of Interest List Accuracy

The LEA supplying a VOI list to the NAS must ensure that information within the list is accurate, of current relevance, and is in a format that conforms to the requirements detailed within TSpec. All lists that are supplied must be reviewed on a regular basis by the LEA supplying the list.

8.13.6. Vehicle of Interest List Deletion

A list that is received from an LEA will be deleted from the NAS no later than 28 days after the last date of revision by the LEA that supplied the list.

8.13.7. Vehicle of Interest List Extraction

LEAs will not extract data from a list of VOI for the purposes of creating a composite list from a number of such lists, to be held outside the NAS.

8.14. Performance Evaluation

Performance testing must be consistent with current guidance provided by the Defence Science and Technology Laboratory (DSTL). (DSTL Guidance)

8.14.1. Installation of ANPR Infrastructure

Unless the exceptions for covert systems apply, on installation of any component of ANPR Infrastructure compliance with performance standards detailed within NASPLE must be confirmed and recorded.

Compliance with performance standards is required for both initial installation or on re-installation or re-deployment of any ANPR camera or other component.

8.14.2. Capture Rate Assessment

Any assessment of ‘capture’ rate must be based on not less than 250 consecutive vehicles (or a minimum period of 2 hours) displaying a VRM visible to the human eye passing within the field of view for a camera and in the case of a multi-lane system this applies to each lane covered by that system.

8.14.3. READ Rate Assessment

The READ rate for each type of system must be determined for not less than 250 consecutive ‘captured’ Vehicles displaying a VRM visible to the human eye.

Performance must be assessed for daylight and night time conditions. It is advisable to assess for a range of conditions including; bright daylight (dawn); bright daylight (dusk); overcast daylight and night time.

8.14.4. Performance Evaluation Schedules

The performance of all ANPR systems must be regularly reviewed to ensure conformance with the data standards defined in this document. NAS functionality should be used to monitor continued compliance with required ‘capture’ rates.

Compliance with the READ rate for a camera should be reviewed at least annually with a sample of not less than 250 consecutive reads. Provisions for performance evaluation must be defined in LEA policy and procedures.

In addition to the annual assessments, the performance standards for all cameras that do not have the capability to provide supporting imagery must be evaluated at no less than 6 monthly intervals. Assessments for this additional assessment shall include a sample of east 50 vehicles passing consecutively within the field of view.

8.14.5. Performance Evaluation of Covert Cameras

Where covert installation of ANPR infrastructure has been authorised within the provisions of RIPA or RIPSA, and the purpose of the installation may be compromised as a result of testing, the testing need not be completed.

8.14.6. Performance Evaluation Logs

A log for all performance evaluation activities must be retained in a form to enable the record of reviews for each component within ANPR systems to be identified and retrieved when required.

9. Part 3: Data Access and Management Standards

9.1. Data Access and Management Standards Overview

Part 3 prescribes the standards required for access to and management of ANPR data within the NAS.

The obligations that arise under the DPA are different depending on the reason for processing of data. It is the responsibility of the controller for the LEA that is processing the data to ensure compliance with relevant parts of the DPA in each case.

9.2. Data Management

9.2.1. Policy

All LEAs that connect to, or have access to, the NAS must have an up to date written policy in place for the access, management and use of ANPR data, including provisions for audit, which must be consistent with Compliance and Audit Standards.

Access to ANPR data must be proportionate to the circumstances of that access and taking account of the impact on the fundamental rights and freedoms of individuals.

9.2.2. Data Access Management

Authorised members of LEAs may access and use data within the NAS to the extent that is compliant with the DPA in the circumstances of each case, without reference to a controller unless otherwise required within the terms of NASPLE.

9.2.3. Shared Collection Equipment

9.2.3.1. Data provision by non-LEAs

NAS may receive data via an LEA from ANPR systems not directly within the control of the LEA in circumstances where it is using shared collection equipment that is owned and managed by a non-LEA organisation.

In these circumstances, the controller for the LEA that initially receives the data and the organisation owning the collection equipment are both controllers who will store data in separate databases that they manage independently. LEA controllers for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user of the shared collection equipment.

9.2.3.2. Data received directly into NAS

NAS may receive data directly from ANPR systems not within the control of an LEA in circumstances where data is submitted to the NAS using shared collection equipment that is owned and managed by a non-LEA organisation, without the data first being received by a LEA.

The NPCC policing lead for ANPR as controller for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment

9.2.3.3. Management of data provided by non-LEAs

In circumstances where a non-LEA has provided data to the NAS, the NPCC policing lead for ANPR and the organisation owning the collection equipment are both controllers who will store data in separate databases that they manage independently.

The NPCC policing lead for ANPR as controller for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment.

9.2.3.4. Compliance Agreement

The LEA that receives data from a non-LEA organisation for submission into NAS, or the NPCC policing lead for ANPR in respect of data submitted directly to NAS, must ensure that a formal written-agreement is in place with the owner of the camera and other components of the ANPR infrastructure detailing appropriate arrangements to enable compliance with NASPLE.

9.2.4. Data Extraction from NAS

Where an LEA accesses data within the NAS they are controller for any data extracted from the NAS as a result of that access. Management of all data that is extracted must be in accordance with the provisions within NASPLE and any reports or other documents that include data from NAS must be marked in accordance with the requirements of the Government Security Classifications (GSC). Personal data must only be processed in accordance with the DPA.

9.3. Organisational and User Access to ANPR Data

9.3.1. ANPR Password Policy

Password requirements for access to NAS is based on national Cyber Security Centre guidelines and is applicable to all roles within LEA, third party contractors and suppliers and staff responsible for NAS service management.

Staff will be allocated individual accounts that may only be accessed using a password in a format approved by the national Accreditor to requirements detailed in Appendix A

9.3.2. ANPR Account Management

Staff who are approved to access NAS as both a user and for administrative purposes must be allocated separate accounts such that these functions cannot be achieved using a single log in account. Accounts must be reviewed, suspended or terminated in the following circumstances:

- An account must be suspended if it is not accessed for a period of 90 days. The need for access must be reviewed within the subsequent 7 days. The account may then be reactivated or deleted as appropriate,

- Access permissions must be reviewed within 7 days of a person changing role within an LEA.

- An account must be terminated within a maximum of 48 hours of a person leaving an LEA or partner agency.

9.3.3. Provisions for Data access

Any access to data must be for national security, counter terrorism, investigation and enforcement purposes as defined in Annex B or for the purpose of audit.

Staff within an LEA may be granted access to the extent relevant to their role, in accordance with local LEA policy in an LEA. LEA policy must be consistent with the purposes and standards within this document and the specific requirements at Annex C.

9.3.4. Data Access provision when NAS is unavailable

Data held within the local components of the NAC (Section 8.9) may only be accessed by authorised staff in circumstances where the NAS or communications to the NAS have become unavailable.

9.3.5. Vetting Requirements for access to ANPR data

Staff accessing the NAC are required to have successfully completed vetting to the standards as detailed below unless in exceptional circumstances with express written approval of the NPCC Policing lead for ANPR, as lead controller, approves any vetting process as equivalent to the required standard.

9.3.5.1. Police

Staff within a police service LEA authorised to access ANPR data must have successfully completed Recruitment Vetting (RV) to NPCC vetting standards.

9.3.5.2. Non - Police LEA

Staff within an Approved Organisation that is a non-police LEA authorised to access ANPR data must have current vetting clearance to national non-police personnel vetting (NPPV) Level 2.

9.3.5.3. Partner Agencies

Controllers may allow access to non-police staff in partner agency (e.g. local authority controllers) subject to have them having current vetting clearance to NPPV Level 2, to the extent necessary for their role.

9.3.5.4. Police Service Administration, Monitoring and Audit

Police LEA staff conducting activity in respect of administration, monitoring and audit of the NAS will have a current security clearance to SC level and NPPV to Management Vetting standard.

9.3.5.5. Non-Police LEA Administration, Monitoring and Audit

Non-police LEA staff conducting activity in respect of administration; monitoring and audit of the NAS will have a current security clearance to SC level and NPPV Level 3.

9.3.5.6. National Audit

Staff appointed to any National Audit role must have a minimum current security clearance to Developed Vetting (DV) level and NPPV Level 3.

9.3.5.7. National Administration and Processor Companies

Staff within NAS supplier companies or the Home Office that have access to the NAS for management or administrative purposes will have a current security clearance to SC level and NPPV Level 3.

9.3.6. Authorisation Requirements for access to NAS Data

Where an authorisation for access is required, staff providing 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.

9.3.6.1. Authorisation of Staff Access

Each LEA will designate a senior manager who is accountable for the authorisation of staff who may access ANPR data.

9.3.6.2. Role Based Access and Training

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 have completed any required training and are fully aware of the provisions within NASPLE. Authorised staff will have individual access accounts and permissions.

9.3.6.3. Records of Authorised Staff

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

9.4. Disclosure and Evidential Use of Data

Data held within or obtained from the NAS may not be used or disclosed for any purposes except those as authorised within NASPLE.

9.4.1. Disclosure schedules

Where ANPR data obtained is retained as material within the meaning of the CPIA (or similar procedures in Scotland), in preparation of disclosure schedules, information relating to ANPR methodology, tactics and camera locations will be recorded on the Schedule of Sensitive Material and may be disclosed to prosecution authorities.

9.4.2. Restrictions on personnel in disclosure of ANPR and in production of evidential materials

Statements of evidence in respect of data within the NAS may only be provided by staff authorised within LEAs to provide ANPR evidence with current access permissions within NAS for that purpose. Subject to the following authorised staff may provide a statement of evidence for any data held within the NAS.

9.4.3. Provisions to safeguard the location of ANPR infrastructure

The order to safeguard the national ANPR infrastructure, apart from data obtained from a Mobile ANPR system, the precise location for an ANPR read obtained from a camera will not be disclosed during an investigation, nor included in evidence unless the controller with responsibility for the camera that recorded the data has been consulted and provided written consent for that disclosure or for evidence to be provided. The following principles apply:

9.4.3.1. Evidential Use of Data

Evidence of an ANPR read will only be included where it is of specific relevance to an investigation and is of material value to any judicial proceedings.

9.4.3.2. Disclosing of Camera Locations in Evidence

Apart from data obtained from a Mobile ANPR system the production of a map or otherwise disclosing the precise location of the camera that recorded an ANPR read is not permitted during any stage of an investigative or prosecution process, unless specifically authorised by the data controller for the LEA with responsibility for the camera that recorded that data.

9.4.3.3. Information to be included in evidential disclosure

The location of a read will be described in the following decreasing order of preference;

1. The general area of the location (e.g. Town, District, Metropolitan Borough)

2. The postcode (following consultation with the controller with responsibility for the camera that recorded the data, in circumstances where this will identify the precise location of the camera)

3. The name of the road (following consultation with the controller with responsibility for the camera that recorded the data, in circumstances where this will identify the precise location of the camera)

4. The precise location (following consultation with the controller with responsibility for the camera that recorded the data)

9.4.3.4. Disclosure of ANPR data for non-evidential purposes

Unless permitted within section 9.6 of this document, core ANPR read data and any supporting imagery as defined by section 7.4.5., is not to be transferred to other systems, nor disclosed to any third party, including staff from an organisation that is not listed at Annex A, Data may only be disclosed to the data subject in accordance with procedures for dealing with FOI and DPA enquiries in accordance with section 9.12. Data may be shared with an organisation that is not listed at Annex A with the express written authority of the controller with responsibility for the camera that recorded that data.

9.4.3.5. Disclosure to non-Approved Organisations

Where an LEA has an active role in collaboration with another LEA which is not listed at Annex A in the conduct of an investigation, and circumstances consistent with the provisions of Schedule 2 DPA apply, 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 controller for the ‘Approved Organisation’ collaborating in the investigation.

9.4.3.6. Controller Representations re Disclosure of Camera Locations

In addition to the above, the controller that owns or controls the camera that captures ‘read’ data will be provided with a specific opportunity to make representation to any court that is to consider an order for information to be disclosed regarding the location of a camera.

9.4.3.7. Recording of Disclosure

In all circumstances where data is disclosed a record must be maintained to include the identity of those disclosing and receiving the data and the reason for and any authorisation of that disclosure.

9.5. Retention and Deletion

9.5.1. Record Retention and Deletion

ANPR READ records must be deleted 12 months[4] after their initial capture, unless retained under provisions of CPIA or similar provisions in Scotland. Retained data may only be accessed in connection with the investigation subject to that retention after a period of 12 months following initial capture.

Records may also be retained for longer than 12 months following a review that identifies a continuing policing purpose for those items of data under provisions of MOPI. These records must be retained and managed in accordance with those provisions. LEAs must establish procedures for the management and review of any data held under these provisions including arrangements for deletion as required.

9.6. Storage of ANPR Data otherwise than in NAS

Data must not be stored outside the NAS except where held in buffer storage in accordance with section 8.9.5 unless for the purpose of retention in accordance with section 9.5.1 or in accordance with section 9.8 below where those requirements cannot be met within the NAS, or it has been extracted as a result of a court order or other lawful authority for the provision of the data.

9.7. Record Amendment

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

9.8. Record Deletion from Third Party Systems

ANPR data must be deleted from any computer-based system within 7 days of entry of that data, where an LEA has established any link between the NAS and any other computer-based system for the purposes of:

- Monitoring and the initiation of an operational response to any hit against a list of vehicles of interest or

[4] Read metadata is deleted on day 366 after initial capture. Associated images are deleted the following day. Data may only be accessed up to 12 months after initial capture (Annex C) unless in circumstances of 9.5.1 above.

- More advanced research and analysis purposes in relation to an investigation.
- Entries are included in command and control records

An exception exists for deletion after 7 days when a review has been conducted of the data that it is proposed to be retained which has identified the items of data where a continued policing purpose remains that can only be satisfied by the continued processing of the data within the system external to the NAS.

In this case provisions of MOPI (or similar provisions in Scotland) apply and the relevant items of data may be retained and managed in accordance with those provisions; or

An exception also exists for deletion after 7 days when a review has been conducted into the data that it is proposed to be retained which has confirmed that the items of data are relevant to an investigation. In this case the relevant items of data may be retained, managed and deleted in accordance with the requirements of CPIA.

9.9. Transfer to local systems for basic user access

Data may not be transferred to any local systems external to those required for connection to NAS facilitate basic user access to ANPR data.

9.10. Records of Data Processing, Access and Disclosure

9.10.1. NAS Logging

A log of all automated processing operations will be maintained within NAS to include records of access by administrators and authorised users, data capture, alterations and any search of data or records within NAS. Logs of administrator or user access must include details of the identity of the user together with the justification, date and time of that access and a record of any authorisation relevant to that access.

9.10.2. Mobile Systems Logging

A log recording the details of all lists of VOI that have been loaded onto mobile systems as authorised by section 8.9.8 will be maintained by the LEA that loaded the log onto the mobile systems.

9.10.3. Logging of Access on systems external to NAS

In addition, LEAs are required to maintain a record of any access by their staff to ANPR data, in any external system, to include records of access by administrators and authorised users, data capture, alterations and any search of data or records within NAS. Logs of administrator or user access must include details of the identity of the user together with the justification, date and time of that access and a record of any authorisation relevant to that access in a readily retrievable form.

9.10.4. Logging of Escalation of Investigation Category

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.

9.10.5. Logging of data Disclosures

Unless disclosure is in accordance with the provisions of the CPIA or similar provisions in Scotland, LEAs will maintain records of all disclosure of ANPR data including the justification, data and time of the disclosure, the identity of the person disclosing the data and the identity of the recipient of the data.

9.10.6. Use of Logs in Disciplinary Proceedings

Logs within NAS and those recorded by an LEA may be used for the purposes of self-monitoring by the controller or the processor, the conduct of internal disciplinary proceedings, in ensuring the integrity and security of personal data and for the purposes of criminal proceedings.

9.10.7. Disclosure of Logs to ICO, SCC and Home Office

Records within NAS and any local records must be made available to the Information Commissioner, the Surveillance Camera Commissioner and the Home Office on request for audit and monitoring purposes.

9.11. Management and Audit of NAS

Audit must be conducted in accordance with National Standards for Compliance and Audit of Law Enforcement ANPR by staff with appropriate security clearance.

LEAs will support all controllers for NAS in the audit and management of NAS.

LEAs will support the national auditor in the monitoring and audit of access to the NAS and will provide relevant information on request.

LEAs will audit the access to NAS by their staff in accordance with Audit Standards and maintain a record of all audits that are undertaken. Details of such audits will be made available to the Information Commissioner, the Surveillance Camera Commissioner and the national auditors on request.

9.12. Freedom of Information Act and Data Protection Act Enquiries

All requests for Information regarding the NAS made to a public authority under the provisions of the Freedom of Information Act 2000 (FOI) will be referred to the relevant controller for consideration and will be managed according to the JCA.

All requests in relation to data held on NAS, made under provision of the DPA, will be referred to the controller for consideration and will be managed according to the

JCA. This includes any subject access requests and requests for erasure or restriction on processing.

Annex A: Approved Organisations

List of Approved Organisations
Avon and Somerset Constabulary
Bedfordshire Police
Border Force
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Civil Nuclear Constabulary
Cleveland Police
Cumbria Constabulary
Department for Work and Pensions (DWP)
Derbyshire Constabulary
Devon and Cornwall Constabulary
Dorset Police
Driver and Vehicle Licensing Agency (DVLA)
Driver and Vehicle Standards Agency (DVSA)
Durham Constabulary
Dyfed-Powys Police
Environment Agency
Essex Police
Food Standards Agency
Gangmasters and Labour Abuse Authority
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
H M Revenue & Customs (HMRC)
Humberside Police
Immigration Enforcement
Intelligence Services
Kent Police

Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Medicines and Healthcare Products Regulatory Agency (MHRA)
Merseyside Police
Metropolitan Police Service
Ministry of Defence Police
National Crime Agency (NCA)
NAFN Data and Intelligence Services facilitating Local Authority Trading Standards investigations
National Vehicle Crime Intelligence Service (NaVCIS)
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
Police Service of Scotland
Police Service of Northern Ireland (PSNI)
Royal Air Force Police
Royal Military Police
Royal Navy Police
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police
Thames Valley Police
Thurrock National Investigation Service
Warwickshire Police
West Mercia Constabulary
West Midlands Police
West Yorkshire Police
Wiltshire Police

Annex 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

Major Investigation Types
Murder
Attempted Murder
Manslaughter
Infanticide
Child Destruction
Kidnapping

Terrorist related crimes

Serious Investigations

Designated Serious Investigations

Serious Investigation Types
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/ public security

Serious Investigation Escalation

Serious Investigations may, with the authority of a senior manager[5] 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:

Serious Investigation 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

[5] an officer of at least superintendent rank in the police or the equivalent level of seniority in a non-police organisation

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. This will include investigations into street robbery, burglary and vehicle-related criminality and non-crime issues such as anti-social behaviour, vehicle excise enforcement, road traffic offences, safeguarding and missing persons.

Priority and Volume Investigations may with the authority of manager[6], 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:

Priority and Volume Investigations Escalation Factors

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

[6] an officer of at least Inspector rank in the police or the equivalent level of seniority in a non-police organisation

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

Annex 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.
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.
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.

	To research data for 'National Security', 'Counter Terrorism' or other 'Major Investigation' purposes.
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.
	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.

Appendix A: Password Requirements

Password Requirements

Introduction

Purpose

1. The security of NAS requires that users generate an appropriately complex password to protect the National ANPR Capability (NAC) and its data from unauthorised access. The NAS utilises a username and password-based identity and access control for all front-end users.
2. The NAS Password Policy is a procedural part of the information security measures intended to:
   - Protect the Confidentiality, Integrity and Availability of the NAC.
   - Preserve the privacy of all the data and information stored within the NAC environment, ensuring only authorised users are permitted access on a need to know basis.

Procedures

The Purpose of Passwords

3. Passwords are an essential security control to authenticate users and confirm identity and access rights. Passwords protect access to the ANPR data and information in conjunction with the physical and procedural measures of a secure site.
4. Visual recognition of people within a work area, and Photographic ID Cards for sites and buildings, are also an important security layer to protect the NAC.

Limitations

5. The security provided by a password system requires the passwords are known only to the user of the account to which it relates. Thus, a password is vulnerable to compromise whenever it is stored or written down. A user must not disclose their password to anyone including other users and administrators.

Password Requirements

Password creation requirements:

6. Passwords **must** be a minimum length of 8 characters with at least 2 non-alphanumeric characters (e.g. % & ?);
7. Passwords **must not** be stored in any insecure form, users must **disable** password saving in web browsers;
8. Passwords **must not** be based on the following:
    - Months of the year, days of the week or any aspect of dates with which they are personally associated (e.g. birthdays, anniversaries);
    - Family names, initials or car registration numbers;
    - Organisation names, identifiers or references;
9. Good quality passwords should:
    - Not be the same as any of the previous 10 passwords (this will be enforced via the operating system or security solution within NAC);
    - Be unique and only used within the NAC;
10. Password must be changed on suspicion of compromise;
11. Password creation requirements are common for all types of NAC access. If a user has more than one account. For example, a user administrator and system administrator account, different passwords are required for each account;

Expiry terms and Account Lockout

	No of Attempts	*Password expiry*
User/ Role	5	1yr

12. If a user has attempted to log in **5 times** unsuccessfully their account will be:

    a. **Locked out** and **ONLY** unlocked via two alternative processes for use depending upon the business processes of the LEA:
        i. Notify the local User Administrator or,
        ii. Notify the local LEA IT Service Desk.

Forgotten Password Process

13. If a user has forgotten password, A **"I forgot my password"** link is provided on the NAS logon homepage. The system will email a new temporary password to the email address associated with the NAS user account. This temporary password **must** be immediately changed upon first successful login. This will not circumvent the lockout procedure described above.

This publication is available at www.gov.uk/government/publications and www.npcc.police.uk/anpr

Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk .