



Automatic Number Plate Recognition (ANPR) POLICY

Table of contents

Table of contents	1
Section 1	1
Section 2	1
Section 3 – Procedural guides.....	5
Section 4 - Relevant Legislation:	6
Section 5 – Related References:.....	6
Section 6 - Identification, Monitoring and Review	7

Section 1

Gloucestershire Constabulary Automatic Number Plate Recognition (ANPR) Policy

Automatic Number Plate Recognition (ANPR) technology can and does help detect, deter and disrupt criminality at a local, force, regional and national level, including tackling traveling criminals, Organised Crime Groups and terrorism.

Such is the value of ANPR as a tactical option providing new lines of enquiry and evidence in the investigation of crime it is now well established through England, Wales, Scotland and Northern Ireland.

Investigators in local and cross border criminality and Senior Investigating Officers in cases of terrorism, organised and other major crime are increasingly reliant on ANPR to provide cost effective support to investigations.

Gloucestershire Constabulary ANPR Strategy

“To deliver a technical ANPR infrastructure that provides a force capability to detect vehicle movements in and around key locations. Thereby enabling effective data collection and analysis which facilitates an improved investigative and intelligence capacity for the force.”

Section 2

National ANPR Standards for Policing (NASP) describe the standards that are required to be met for the development and use of ANPR systems by Law Enforcement Agencies (LEAs).

The policy for the development and use of ANPR within Gloucestershire Constabulary is that it is consistent with NASP and this document outlines accountability and responsibility in that regard.

National ANPR Standards for Policing (NASP) can be found on the **FIB Intranet Site – Policies**

2.1 Strategic Leadership

The Chief Officer lead is ACC Operations

The Strategic Lead is Det. Supt. Intelligence & Covert Policing

The Operational Leads are – (1) Intelligence & Investigations

DCI Intelligence & Specialist Crime



Automatic Number Plate Recognition (ANPR) POLICY

(2) Technical Support

ICT Chief Information Officer

(3) Operational Response

Supt, Incident Management

2.2 Infrastructure Development and deployment of Number Plate Reading Devices (NRD)

Infrastructure Development will be in accordance with Home Office (HO) Procedure for the Development and Review of ANPR Infrastructure.

Proposals for new infrastructure will be submitted to the Strategic Lead who is responsible for confirming that the proposals are appropriate and proportionate, taking account of strategic assessment and privacy impact assessment, in balancing protection of the public with the rights and legitimate expectations of individual privacy. That confirmation is required before any development is progressed.

The Strategic Lead will ensure that arrangements are in place for review of the locations of all Number Plate Reading Device (NRD) that submit data to the ANPR system at least annually to ensure that the deployment remains appropriate and proportionate.

Vehicle mounted ANPR systems will be deployed in accordance with NASP Part 2 standards for deployment of 'Vehicle - Mounted Systems'.

Any deployment in support of operational response following the report of a crime or incident can be made on authority of the Force Incident Manager (FIM) within the Force Control Room and a record of that authority will be made within the incident log.

2.3 Databases

The PNC is the primary database to support operational response. Whenever possible the 'live' PNC link will be used. The PNC extract file is provided three times every 24 hours.

The ANPR manager will ensure that it is loaded onto the ANPR system upon receipt.

Within the PNC files the ACTION (ACT) and Stolen (LOS) reports are the primary databases. ACT reports are designated as High, Medium and Low priority

These databases will be used for the circulation of any vehicle of interest that meets the criteria within the PNC Business rules and will be monitored 24/7 within the Force Control Room and resources deployed as appropriate..

Monitoring of the PNC Reports will be in accordance with the Force Control Room Back Office Facility (BOF) Monitoring Policy.

A local list of vehicles of interest (VOI) may be used to circulate vehicles for intelligence monitoring purposes or in circumstances that do not meet the standards for inclusion on the PNC as an ACT report for operational response.

Local lists of VOI may be circulated to another LEA to support cross border activity or in support of a specific operational activity. These lists must not be circulated nationally.



Automatic Number Plate Recognition (ANPR) POLICY

The member of staff (ANPR SPOC/Vehicle Intelligence Officer) who creates a list of VOI will ensure that the information within it is accurate, of current relevance and in the format prescribed within NASP.

The ANPR manager will monitor the creation, use and maintenance of local lists of VOI for operational response purposes, reporting concerns to the Strategic Lead as appropriate.

The Strategic Lead will ensure that arrangements are in place, to monitor the creation, use and maintenance of a list of VOI for intelligence monitoring purposes.

2.4 Performance Evaluation

The ANPR Manager is responsible for monitoring the performance of all components of the ANPR Infrastructure.

The performance of NRD will be assessed on installation and thereafter at least annually for all NRD that provide supporting imagery and every 6 months for any that do not provide images in accordance with NASP Part 2 Para 12.

2.5 Data Access

The Strategic Lead is accountable for the authorisation of staff that may access ANPR data. The strategic lead will ensure that a record of authorised staff is maintained and that authorisation is reviewed, amended or cancelled on change of role as appropriate.

Staff may only be granted access to ANPR data to the extent that is necessary for their role.

Staff accessing ANPR data must ensure that the access is appropriate in each case taking account of NASP and that it has been properly authorised when required.

Staff authorising access to ANPR data must ensure that access is proportionate and in the interest of justice in each case taking account of the Data Protection Act, NASP data access provisions, Investigation Categories and Search Authorities.

ANPR Investigation Categories and Search Authorities can be found on the **FIB Intranet Site – Procedures**

2.6 Evidential Use and Disclosure of Data

ANPR data and images are initially for intelligence purposes only. Images or reads may not be used evidentially without written permission of the data owner.

The designated ANPR SPOC/Vehicle Intelligence Officer (VIO) within FIB will be consulted before preparation of disclosure schedules under Criminal Procedure and Investigations Act 1996 (CPIA) provisions and before any ANPR data is used as evidence in any proceedings.

The ANPR SPOC/VIO will also facilitate liaison with other Forces ANPR Managers prior to disclosure of any outside Force ANPR data as appropriate.

The disclosure of ANPR methodology, tactics and camera locations will be avoided whenever possible in order to ensure the continued value of ANPR as an operational and investigative capability. Concerns regarding disclosure or evidential use will be referred to the ANPR SPOC/VIO for consideration.



Automatic Number Plate Recognition (ANPR) POLICY

Statements of evidence may only be provided by the ANPR SPOC/VIO.

During the course of an investigation, ANPR images; Investigation methodology; tactics, or maps indicating the locations of ANPR cameras will not be disclosed to suspects or their legal advisors without the approval of the ANPR SPOC/VIO.

The ANPR SPOC/VIO will advise investigators on the information that may be revealed in each case. In respect of locations the options are: (in decreasing order of preference)

- The general area of the location (e.g. City/Town/Area)
- The postcode
- The name of the Road
- The precise location of the ANPR read

Statements of evidence will normally only be prepared after proceedings have been initiated and following a specific request of the Crown Prosecution Service (CPS). However, all requests for evidential use of ANPR data will be referred to the ANPR SPOC/VIO for consideration and authorisation as necessary.

ANPR material not used in evidence will be included on the MG6D Schedule of Sensitive Material.

ANPR Data is subject to weeding (currently 12 months). it is the responsibility of investigating officers to notify the ANPR SPOC/VIO of any further retention requirements

The required Forms to request ANPR data locally and nationally and/or requests for the use of ANPR in evidence can be found on the **FIB Intranet Site - Forms**

2.7 Records of Data Access and Audit

The strategic lead will ensure that provisions for regular audit of access to ANPR data are in place, with a record of all audit activity that has been undertaken.

Where data has been accessed for which the data controller is from another LEA, the data controller will be provided to that data controller on request.

Details of audits undertaken will be made available to the Information Commissioner; the Surveillance Camera Commissioner and the Home Office on request.



Automatic Number Plate Recognition (ANPR) POLICY

2.8 Mobile Data

There are two designated ANPR computer terminals, one located at the Tri-force Operations Centre, Bamfurlong and the other at Stroud, connected to the Forces Network.

These facilitate the process of transferring files between Mobile Data Terminals (MDT) for ANPR/Video images to be transferred from the MDT to the appropriate case files on the network in a controlled manner.

All existing Force Security Policy's will apply to these terminals.

The only authorised USB Memory Device that is permitted for use on Constabulary IT Systems is the Data Traveller Black Box (DTBB) from Kingston Technology.

There are exceptions to the above where non encrypted USB Memory devices for the transfer of data relating solely to ANPR/Video Mobile Data Systems supplied by Clearstone Telecoms PLC have been approved by the Force Accreditor, the Forces Information Security Officer (ISO).

Any unapproved/private owned USB Memory Device discovered in use with MDT equipment or connecting to the network will be immediately confiscated and the user may be subject to disciplinary procedures.

Section 3 – Procedural guides

Not Applicable



Automatic Number Plate Recognition (ANPR) POLICY



Section 4 - Relevant Legislation:

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.

Access to and the retention and management of ANPR data are compatible and consistent with obligations that arise under:

- 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
- 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
- The Surveillance Camera Code of Practice issued under provisions of the Protection of Freedoms Act 2012 (PFA)
- 'In the Picture' – Information Commissioner
- Criminal Procedure and Investigations Act 1996
- College of Policing Approved Professional Practice – Information Management.

Section 5 – Related References:

Not Applicable



Automatic Number Plate Recognition (ANPR) POLICY

Section 6 - Identification, Monitoring and Review

Security Marking:		RESTRICTED		
Document Title: Automatic Number Plate Recognition (ANPR) Policy				
Type		URN	Strategic Board	Author/Reviewer
Policy		269		Andy Evans ANPR Manager Force Intelligence Bureau Ext 2612
Version	Date	Changes (ensure public copy amended and uploaded to external website)		Complied with Policy Guidance ✓
V1.0	1/12/16			✓
V1.1	12/12/16	Updated FCR Monitoring Policy (V1.6)		
V1.1a	6/9/2017	FOI version created.		
V2.0a	8/5/18	Insert section 2.8 (mobile data) and update data retention period (12 months)		
Next Document Review Date: 12/12/2017				
EIA		EIA Sign Off		EIA Review
LOW/MEDIUM/HIGH				
SIA		SIA Sign Off		SIA Review
<i>This version will be placed on the public domain website</i>				
If this version cannot be placed on the public domain website, provide reason and relevant COG authority				

Previous policies can be found with the continuous improvement team.