



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

Response Date: 11/06/2025

2025/553 - DPIAs

In response to your recent request for information regarding;

1. All completed Data Protection Impact Assessments (DPIAs) currently in force that relate to:

- **Recording, retention, and disclosure of audio-visual material obtained through such BWV devices;** none held
- **The processing of personal data in custody suites, including verbal interviews, searches, photographs, and fingerprints;** none held
- **The use of automatic number plate recognition (ANPR) and vehicle surveillance technologies;** please see attached.

Concerns have been raised in relation to providing the appendix which lists locations. Therefore, a public Interest Test has been carried out to weigh up the reasons for and against disclosure; to ensure the release is in the interest of the public as a whole and not just the applicant.

Section s31(1)(a)(b) Law Enforcement

Section 31 (1)(a)(b) is a prejudice based qualified exemption, therefore there is a requirement to articulate the harm that would be caused in confirming or not that the information is held as well as carrying out a public interest test.

The Harm Test process requires North Wales Police to consider any possible harm that might arise as a result of placing the requested information into the public domain. This process considers the potential harm to:

- Individuals
- The community as a whole
- North Wales Police and the wider policing service
- Other bodies

S31(1) - Evidence of Harm

A Freedom of Information Act request is not a private transaction. Both the request itself and any information disclosed, are considered suitable for open publication. This is because under the Act, any information disclosed is released into the wider public domain, effectively to the world, not just to an individual.

Whilst not questioning the motives of the applicant, providing exact locations of the ANPR would make them less useful.

Pencadlys yr Heddlu,
Glan-y-Don, Bae Colwyn LL29 8AW
www.heddlugogleddcymru.police.uk

Police Headquarters,
Glan-y-Don, Colwyn Bay LL29 8AW
www.northwales.police.uk

ANPR are vital in many investigations, if locations are widely known persons trying to evade detection would evade the locations of the cameras making our law enforcement more challenging.

There is always a duty of care to the general public and the Police Service has a clear responsibility to ensure the prevention or detection of crime, and the apprehension or prosecution of offenders is always delivered. There are a number of tactics available to the Police Service to ensure the effective delivery of operational law enforcement.

As such, the disclosure of any further information which would hinder the forces law enforcement functions cannot be in the public interest.

Public Interest Test

Factors favouring disclosure for S31 - Where public funds are being spent, there is a public interest in accountability and justifying the use of public money. Disclosure of the requested information would enable the public to assess whether the force has appropriately taken steps to help reduce crime by such means as the use of technological assistance. Release would enhance public debate as to whether or not the force is appropriately and effectively engaging with the threat posed by the criminal fraternity.

Factors against disclosure for S31 - Disclosure that reveals our ANPR locations would compromise law enforcement tactics. Criminals could use the information to evade areas of detection. It may be used by criminals who are intent on pursuing their criminal activity, to identify and exploit the limitations of these resources.

Any disclosure of information which would compromise law enforcement tactics and thus lead to more crime being committed by reducing the opportunity for the prevention and detection of crime, would therefore increase the risk to public safety, which is not in the public interest.

Balancing Test

Law enforcement is of paramount importance and the Police service will not disclose information if to do so, it would undermine its purpose and place the safety of individual(s) at risk. Whilst there is a public interest in the transparency of using public money in policing appropriately and effectively engaging with the threat posed by criminals, there is a very strong public interest in safeguarding the integrity of police investigations and operations in this area.

As much as there is public interest in knowing that policing activity is appropriate and balanced in matters of law enforcement, this will only be overridden in exceptional circumstances. The use of ANPR is vital in many investigations, it is a police tactic that is open to police forces for the purpose of law enforcement and can assist in the prevention and detection of crime. Any disclosure which hinders our capability and assists criminals cannot be in the public interest.

It is for these reasons that I have determined that the balance test favours non-disclosure of the requested information.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

- **Any DPIAs relating to execution of search warrants, Section 8 PACE entries, or surveillance linked to property-based investigations;** none
- **Any generic DPIAs governing operational policing within private or domestic premises.** None

2. Where no DPIA has been completed for any of the above processes, please confirm this explicitly and state: This isn't information held.

- **Whether a DPIA is currently in development or under internal review;** as above
- **If so, the estimated completion date and the officer responsible for that review.** as above

3. **A copy of any ROPA (Record of Processing Activities) entry related to BWV, property-based investigations, or arrest-related surveillance.** – spreadsheet attached
4. **A copy of North Wales Police's BWV policy, including provisions regarding:**
 - **Activation thresholds and officer discretion;**
 - **Use of BWV during arrests, interviews, and inside homes;**
 - **Disclosure and redaction practices;**
 - **Audit logging, retention, and sharing with third parties (e.g. CPS, defence).**

Please find attached

5. **A copy of the privacy notice provided to data subjects (e.g. suspects or civilians) when BWV is activated during arrests or residential enforcement.**

There isn't a specific one, this would be covered by the Force one ;

[Privacy Notice | North Wales Police](#)

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 09/06/2025

OFFICIAL

Automatic Number Plate Recognition (ANPR)
Data Protection Impact Assessment



CS - SURVEILLANCE
NEW.xlsx

NORTH WALES POLICE

Automatic Number Plate Recognition (ANPR) National ANPR Service (NAS) Data Protection Impact Assessment (DPIA)

Owner: Temporary Detective Superintendent...

Author: ...

Time Period Covered: From February 2025 (Review Date February 2026)

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 1 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

CONTENTS	Front Page	1
	Contents	2
1	Acronyms	3
2	Introduction	4
3	Purpose of ANPR Data Protection Impact Assessment	5
4	Description of recent ANPR development in North Wales	6
4.1	Northgate Back Office Facility (BOF)	6
4.2	National ANPR Data Centre (NADC)	7
4.3	National ANPR Service (NAS)	7
4.4	Vehicle Intelligence Server and Communications Engine (VISCE)	7
4.5	Analytical capability provided by the National ANPR Data Centre (NADC)	7
4.6	IAC Mobile phone ANPR Application	8
5	The need for an improved ANPR service	8
6	The need for a National ANPR Service	9
7	How ANPR has improved with the introduction of NAS	10
7.1	Disparate Legacy Systems	10
7.2	New Capability and Functionality	10
7.3	Supporting Investigations	10
7.4	Humans Rights Compliance	10
7.5	General Data Protection Regulation (GDPR) compliance	10
7.6	Data Protection Compliance	10
7.6.1	Data Retention	10
7.7	National ANPR Strategy	10
7.8	Success criteria for NAS	11
8	Identifying the need for a DPIA	11
9	Why do we need another DPIA?	11
10	Processing ANPR data	12
10.1	Nature of Processing	13
10.2	Scope of Processing	14
10.3	Context of Processing	15
10.4	Purpose of Processing	16
10.4.1	Strategic Goals.	16
10.4.2	Organisational Context	17
10.4.3	Economic and Financial Environment.	18
10.4.4	Operational Maturity	18
10.4.5	Privacy and Transparency	19
10.4.6	Capability Support to Law Enforcement Agencies	19
10.4.7	Infrastructure Development	20
11.	Consultation Process	21
11.1	Internal Consultation	21
11.2	External Consultation	23
12	Necessity and Proportionality	24
13	Collateral Intrusion	26
14	Social Pressing Need	27
15	Identify and assess risks	29
16	Identify measures to reduce risk	30
17	Sign off and record outcomes	34
Appendix i	Appendix i North Wales Static ANPR Camera Capability	35
Appendix ii	Appendix ii North Wales Mobile ANPR Capability	46

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 2 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

1. Acronyms	
ANPR	Automatic Number Plate Recognition
APN	Access Point Name
BOF	Back Office Facility (Northgate ANPR System)
CPIA	Criminal Procedure and Investigations Act
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
OCG	Organised Crime Group
ICO	Information Commissioners Office
LEA	Law Enforcement Agency
MOPI	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.
NADC	National ANPR Data Centre
NAI	National ANPR Infrastructure -A network of ANPR cameras, communications links, firewalls and other related supporting components
NAS	National ANPR System/Service
NASPLE	National ANPR Standards for Policing and Law Enforcement
NDI	NDI Technologies - Company name
NPCC	National Police Chiefs Council (previously ACPO)
NPIA	National Police Improvement Agency
NWP	North Wales Police
NWROCU	North West Regional Organised Crime Unit
PoFA	Protection of Freedom Act
PIRM	Police Information and Records Management
PNN	Police National Network
QRO	QRO Solutions - Company name
RMS	Record Management System
SCC	Surveillance Camera Commissioner
UK	United Kingdom
VISCE	Vehicle Intelligence Server and Communications Engine
VOI	Vehicle Of Interest
VRM	Vehicle Registration Mark
WTTC	Welsh Transport Travel Consultants

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 3 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

2. Introduction

North Wales Police serves a population of approximately 688,000 people (which is expected to increase to 720,000 in the next twenty years) and covers an area of 6,300 square kilometres. In addition to the local population, North Wales has a high transient population due to its being a popular holiday destination and desired location for second homes. As with most Police Forces there are limited resources available for policing such a large geographical area, especially around the non-arterial routes.

North Wales Police has had Automatic Number Plate Recognition (ANPR) fixed and redeployed sites in Force since 2006. The ANPR fixed sites were funded as part of a National project by the then National Police Improvements Agency (NPIA).

North Wales currently has 62 fixed camera sites, housing over 112 cameras in addition to 38 identifiable police vehicles fitted with ANPR cameras.

The fixed camera locations were chosen based on previous Strategic Assessments and crime patterns of criminals travelling across our borders and throughout North Wales. Areas of focus include those travelling from the Northwest region and passing through Holyhead Port.

The benefit of the current locations continues to be proven on a daily basis through the intelligence and evidential value to investigations, ranging from volume crime through to serious, major and complex investigations.

The use of ANPR has a minimal impact on the community at large as its focus is on those that cause distress to the community by committing local and major crimes.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 4 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

3. Purpose of ANPR Data Protection Impact Assessment

The purpose of this is Data Protection Impact Assessment (DPIA) is designed to support North Wales Police compliance with data protection and human rights obligations and in particular meet individuals' expectations of privacy when developing the ANPR infrastructure.

The DPIA supports the identification of data privacy risks and the template utilised has been developed in consultation with the Information Commissioner's Office (ICO) and the Surveillance Camera Commissioner (SCC), to provide a consistent approach to the conduct of DPIA and support compliance with the requirements of Data Protection Act 2018 (DPA).

ANPR is deployed by the police and other LEAs in accordance with Part 3 DPA, for law enforcement purposes as defined by Section 31 DPA.

The statutory requirement for a DPIA arises under Section 64 DPA and enables the controller to demonstrate that their processing of personal data is compliant with that Act.

The ICO has responsibility for regulating and enforcing data protection law and has published guidance to assist compliance.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 5 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

4. Description of recent ANPR development in North Wales

Historically as ANPR in North Wales developed and as part of the Welsh Government (WG) National Traffic Data Systems Project, many camera sites within the current infrastructure were identified to assist North Wales Police in denying criminals the use of the roads.

These early WG sites are located on the main trunk roads across North Wales including the side routes that benefited the Welsh Transport Technology Consultants (W TTC). As part of the agreements with W TTC they received a sanitised portion of the vehicle number plate data for use in journey time analysis. As a result of this collaboration North Wales Police have benefited from free access to Welsh Government land, fixtures and fibre optic communications.

As part of the development described above, North Wales Police also purchased cameras to cover gaps in ANPR coverage across North Wales.

The Welsh Government technically supported their camera assets utilising their own engineers whilst North Wales Police made use of third party IT support.

For the purposes of this assessment, there are a number of new camera locations to be considered building upon previous DPIA'S causing change to North Wales Police's ANPR Infrastructure.

Furthermore this assessment is able to detail the route of the data from those cameras through to the National ANPR Service (NAS) which caused a huge technical and process change for all forces over the last couple of years.

4.1 Northgate Back Office Facility (BOF)

Historically the ANPR structure in North Wales routed ANPR data from both the static camera infrastructure and the cameras fitted within police vehicles through a firewall into the North Wales Police network and a middleware server. The data passed out through the North Wales Police firewall and on through a Cheshire Police firewall onto the Cheshire server/network at which point the Northgate Back Office Facility (BOF) provided general users access to the data.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 6 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

4.2 National ANPR Data Centre (NADC) and National Strategic ANPR Platform (NASP)

Both North Wales and Cheshire ANPR data passed through the Cheshire firewall onto the Police National Network feeding the data into the National ANPR Data Centre in Hendon. This allowed local users to access National data and likewise other forces to access North Wales and Cheshire ANPR data. The NADC was intended to be decommissioned and replaced by the National Strategic ANPR Platform (NASP) in 2024 however this has been delayed until 2025. The NASP will provide an advanced analytical capability that the NADC had previously provided UK police forces with. Until the NASP is fully functional North Wales Police are still required to forward ANPR data to the NADC, and North Wales continues to support the National ANPR infrastructure via NAS and the NADC.

4.3 National ANPR Service (NAS)

During the period 2020/2021 North Wales Police decommissioned its Northgate BOF. Routing its ANPR data from the all the ANPR static cameras sites and all ANPR cameras fitted within its police vehicles, to a third party Management Server provided by NDI Technologies (part of the wider Dacoll Group). Once the data now leaves the NDI Management Server it passed through a dedicated Cloud hosted service provided in partnership with Digital Transformation Services, Cloud Consulting (ANS) onto the NAS.

North Wales Police general users are now able to research the ANPR data via NAS. This access allows authorised Law Enforcement Agencies (LEA's) in the United Kingdom (UK) to be able to research every other Police Force's local infrastructure from a single interface.

The Home Office coordinates non-police LEA activity and access to NAS.

The ANPR data obtained from all forces is retained on NAS for one year. This allows users to conduct national historical searches over that one year period.

4.4 Vehicle Intelligence Server and Communications Engine (VISCE)

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 7 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Some North Wales Police users are able to access local data (North Wales cameras) for the 7 days prior to a search via the Vehicle Intelligence Server and Communications Engine (VISCE) provided by NDI.

The ViSCE capability provides North Wales Police with a degree of limited operational resilience in the event of any technical issues with NAS.

4.5 IAC Mobile phone ANPR Application

Commencing January 2024 North Wales police began a programme to provide an application on officer's force issued mobile phones which allows them access to a mobile system which provides ANPR alarm notifications and also provides details of the alarm and details of when the same vehicle has activated cameras in the preceding 7 days. There is no facility to search for individual vehicles. The roll out of the application will be to all operational officers and PCSOs and is envisaged to take several months to complete. This will extend the ANPR capability across the force.

4.6 Analytical capability provided by the National ANPR Data Centre (NADC)

With the introduction of the NAS to all forces it was hoped that the NADC based at Hendon would be decommissioned. However NAS in its final release version failed in its obligation to provide an advanced analytical capability that the NADC had previously provided UK police forces with.

In order to retain this advanced analytical capability, police forces had to obtain and/or retain its connectivity to the NADC. North Wales Police, having decommissioned Northgate BOF, had to seek NADC connectivity via the NDI Management Server. This was successfully achieved and North Wales continues to support the National ANPR infrastructure via NAS and the NADC.

5. The need for an improved ANPR service

Law enforcement officers including police and those working in other Government Departments rely on the national collection of ANPR data to detect and disrupt crime, assist with bringing offenders to justice and recovering vulnerable people to a place of safety.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 8 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

ANPR is critical for policing, providing the capability to track local priority crime, assisting with the management of sex offenders, as well as a powerful tool in the investigation of major crime, serious and organised crime and counter terrorism. During this period of austerity, when the targeted management of resources is more paramount than ever before, ANPR provides a vital intelligence tool to assist in this policing and enforcement function.

Since the early Strategic Reviews of ANPR within North Wales there has been a continued need for an ANPR capability. A longstanding ANPR infrastructure in North Wales has been supporting the national and local policing objectives since that review.

The ANPR capability across the country varies; whilst all Police Forces are now connected to NAS some are still using local BOFs with some hesitancy migrating the bulk of their users to NAS.

A number of Police Forces make use of the advanced analytics provided by the NADC. Currently North Wales are obligated to send ANPR data to the NADC however North Wales users do not have access to the NADC data due to not have a compatible back office system and therefore do not have this advanced ANPR analytical capability. The NADC is in the process of being decommissioned and replaced by NASP. When NASP is fully commissioned the back office system North Wales Police currently have in service (VISCE) will allow users to access this data.

6. The need for a National ANPR Service.

- **Common National Processes**

Police Forces and Local Enforcement Agencies (LEA's) within the United Kingdom have to comply with common levels of connectivity, security and the methodology of supplying data to NAS.

- **Compliance within a National Framework**

NAS and ANPR nationally operates under a complex framework of legislation of general application, including the [General Data Protection Regulations \(GDPR\)](#), the [Data Protection Act \(DPA\)](#), 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).

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 9 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Section 29(6) of the [Protection of Freedoms Act \(PoFA\)](#) 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.

7. How ANPR has improved with the introduction of NAS

7.1 Disparate Legacy Systems

The National ANPR Service (NAS) is a 'Cloud' based solution which stores all ANPR data in one national collection, removing the need for over 40 existing separate Back Office Functions (BOF) within police forces and other law enforcement agencies.

7.2 New Capability and Functionality

The NAS has been designed to reliably provide all forces with direct access to the national data set together with new tools, powerful analytics and alerting functions. It is a core part of the drive for greater efficiency and collaboration and has transformed ANPR technology.

7.3 Supporting Investigations

NAS facilitates new ways of working ensuring the protection of the vulnerable and solving crime at a local level in addition to supporting investigations at a national level countering threats from terrorism, serious organised crime and Modern Slavery and Human Slavery

7.4 Humans Rights Compliance

NAS improves forces effectiveness and better demonstrates that its use is proportionate, reassuring regulators, whilst addressing privacy concerns for the public.

7.5 General Data Protection Regulation (GDPR) compliance

Another important consequence of replacing data held locally with a single national data set is that it becomes possible to standardise management of ANPR data and compliance with the newly introduced General Data Protection Regulation (GDPR). Assurance of such a standardised approach was never possible in the historical ways of working with varied approaches to data management across the country.

7.6 Data Protection Compliance

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 10 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

NAS creates a national ANPR system for compliance with the National ANPR Standards for Policing and Law Enforcement agencies ([NASPLE](#)) ensuring compliance with the Surveillance Camera Code of Practice and 12 Surveillance Commissioner Principles.

7.6.1 Data Retention

One of the principles referred to above relates to Data Retention. NAS provides Case Management which is new functionality and is being utilised to ensure that Data Retention requests by officers (requests made in accordance with the Criminal Procedure and Investigations Act (CPIA)) are recorded and a process created surrounding the subsequent and timely deletion of data when it is no longer required.

7.7 National ANPR Strategy

As the development of the NAS across the country progresses, the need for a national service becomes more evident than ever. The implementation of NAS within North Wales is contributing toward the National ANPR Strategy and objectives primarily 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” (S31 DPA) which will include national security or counter terrorism purposes.

7.8 Success criteria for NAS

The success criteria against which NAS is judged will be the evidence of bringing those to justice who cause most harm within our communities and it is apparent that Police forces are already seeing the benefits of the new system in this regard.

Senior Investigating Officers in cases of terrorism, serious organised crime, major crime along with investigators of local and cross border criminality are increasingly reliant on ANPR which provides a cost-effective support to investigations.

The NAS will continue to provide the community of North Wales with confidence and reassurance in crime prevention and reduction.

8. Identifying the need for a DPIA

Automatic Number Plate Recognition (ANPR) technology is used to help detect, deter and disrupt criminality at a local, force, regional and national level, including tackling travelling criminals, Organised Crime Groups (OCG) and terrorists.

ANPR provides lines of enquiry and evidence in the investigation of crime and is used by Law Enforcement Agencies (LEA) throughout England, Wales, Scotland and Northern Ireland.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 11 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

ANPR may only be deployed, following a strategic assessment that identifies a need for ANPR at that location for DPIA ‘law enforcement purposes’ as defined by the Act; *‘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’* which includes for national security and/or counter terrorism purposes.

Whilst the use of ANPR in this way has proved to be important to law enforcement in the detection of many offences, including the solving of cases of terrorism, and in tackling major and organised crime, it is recognised that ANPR captures personal data and that the extent of data collection presents potential risk to the protection and freedoms of individuals.

9. Why do we need another DPIA?

Previous ANPR Data Protection Impact Assessments completed within North Wales have all related to either:

- The inception of the ANPR Infrastructure
- The expansion of that infrastructure in terms of additional cameras
- The decommission of legacy systems and the introduction of the NAS

All of which affect local community privacy.

The NAS is now slowly embedding itself into the North Wales Police ANPR user community but some technical and resource processes still require attention;

For example;

- The NADC will at some point in 2025 be decommissioned and is being replaced by NASP which will allow forces with compatible back office systems to access analytical capability that NAS cannot provide. North Wales police have a compatible system for this function.
- Not all North Wales Police historical Northgate users have migrated to NAS and processes/procedures within some departments to ensure compliance with NASPLE require ongoing support.
- North Wales has introduced new ANPR camera sites obtained from various funding streams and there will be an introduction of additional sites in 2025.
- The Welsh Government has handed ownership of their camera estate over to North Wales Police who now provide 3rd party IT support for maintenance and fault resolution.
- The above changes have coincided with a procurement process which saw QRO Solutions, a third party IT company, manage all the static cameras now owned by North Wales Police. This is in addition to the QRO middleware server handling North Wales’s ANPR data before it passes to the NDI Management Server.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 12 of 46	

**Automatic Number Plate Recognition (ANPR)
Data Protection Impact Assessment**

This particular DPIA is focussed on the above changes to camera estate, IT support, data pathways and management of data via a management server to a hosted, cloud based service and onto a National ANPR System.

Therefore, given the national system and required technical change, there is a need to review existing North Wales Data Privacy compliance and to assess the effects of any privacy intrusion on our community. Notwithstanding the need to incorporate any recent legislative/process changes since the last strategic assessment.

10. Processing ANPR data

10.1 Nature of Processing

Processing data within NAS involves the collection and subsequent use of records for vehicles passing through ANPR cameras and therefore is identified as ‘high risk’.

This is explained further in that the data collected provides a record of the location of a vehicle at a specific time and date along with a direction of travel. This will often also involve an overview of the vehicle, which may of course include imagery of the occupants. When other data is applied such as the make, model and colour of the vehicle from external agencies, this has the potential to reveal personal data in relation to persons associated with that vehicle.

The integration of that data and the national collection of data present a capability to establish the movements of a vehicle through the national network of ANPR cameras over a given period. Analysis and development of such data can potentially reveal associations between individuals.

As a vehicle passes an ANPR camera, its registration number is read and instantly checked against local and national database records of ‘vehicles of interest.’ Police officers can then intercept a vehicle allowing officers to explore further investigative opportunities with its occupants.

A record is stored of all vehicles passing a camera which may, where appropriate be accessed for investigative purposes by approved Law Enforcement Agencies (LEA).¹, These include those for vehicles that are not known to be of interest at the time of the read.

¹ As defined in [NASPLE](#) Part 3

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 13 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Data is stored within the National ANPR Service (NAS) where it is retained for a period of 12 months unless further preserved under provisions of the Criminal Procedure and Investigations Act (CPIA) or similar provisions in Scotland. Unless preserved, data is automatically deleted 12 months after it first entered the NAS.

In addition, a copy of 'read' data is held locally by North Wales for a maximum of 7 days from initial capture. Where a 'read' is submitted to the local components of NAC more than 7 days after the time of capture, it may be retained for no more than 48 hours in local systems and then deleted within the subsequent 24 hours.²

Where there are links between the NAS and other computer-based systems for the following purposes, the ANPR data must be deleted from those systems within 7 days of entry unless retained under provisions of Police Information and Records Management (PIRM) or (CPIA)³

- For the purpose of monitoring a vehicle movement.
- The initiation of an operational response to any hit against a list of 'vehicles of interest'
- Advanced research and analysis purposes in relation to an investigation.

Data shared by North Wales is subject to the provisions of [NASPLE](#) Part 3 Data Access and Management Standards.

10.2 Scope of Processing

The deployment of ANPR cameras enables the collection of vehicle registration marks (VRM) with the associated plate patch in addition to overview images with associated data detailing the time and location for that read.

The data collected does not include any special category data or criminal offence data; however, the data collected will be compared with local and national lists of 'Vehicles Of Interest' (VOI) within the NAS and that will include criminal offence data.

Each camera records details of a VRM at the location of that camera. The volume of data collected is variable due to changing traffic flows at that location however it will be integrated into the NAS where it will be stored with reads from other cameras throughout the United Kingdom (UK). The overall volume of reads submitted to the NAS can exceed 90 million per day.

In North Wales approximately 288 Million reads per year are retained.

² [NASPLE](#) Section 8.9.6

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 14 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Data is stored within the NAS where it is retained for a period of 12 months unless preserved under provisions of the PIRM and CPIA or similar provisions in Scotland. Unless data is preserved it is automatically deleted 12 months after it first entered the NAS.

Geographical issues

The North Wales Police ANPR infrastructure covers 63 static camera sites where 112 cameras are located, also to be included are a number of police vehicles fitted with ANPR capability.

North Wales Police have 24 Road Crime Unit (RCU) vehicles fitted with ANPR and 3 Local Police Service (LPS) vehicles fitted with ANPR. A further 9 LPS vehicles are to be commissioned within 2025 and another 2 LPS vehicles in 2026.

Cameras are strategically placed on arterial routes entering and exiting North Wales. Neighboring Police forces provide a similar infrastructure with their cameras, operating just outside of North Wales' geographical borders and beyond. Together all of these cameras feed into the National ANPR Service.

Critical locations within North Wales which provide a risk in terms of Counter Terrorism include the port area of Holyhead and a high volume of traffic influx from the North West into the Deeside area which sees an increase in the number of cameras at those locations. This increase is to cater for lane control, complex traffic management at junctions and traffic volume at those points, particularly in the summer season.

10.3 Context of Processing

North Wales Police has no direct relationship with individuals whose vehicles are subject of ANPR reads. The data collected relates only to vehicles and can be regarded as unidentifiable at the point of collection as personal data relating to an individual can only be obtained by reference to another data source ie DVLA data.

Individuals within North Wales Police have no control of the collection of data from a location.

The data collected may be linked to the registered keeper of a vehicle or to persons linked with a vehicle in other data storage systems and whilst registered keeper data will not include children it is possible that other data systems may include links to children and vulnerable groups.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 15 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

The use of ANPR for collection of data regarding vehicle movements is established technology and details of the use are published by the LEA on websites and through the National Police Chiefs' Council (NPCC).

The concerns from some members of the public in relation to the potential impact on their data and privacy are recognised. The LEA conforms fully to the requirements of [NASPLE](#) which provides significant safeguards to the granting of user permissions for access, with clear criteria to support proportionate access to the data. Provisions for logging and audit have also been established.

ANPR technology is overt and potentially the public generally do have a lower expectation of privacy when in/on a vehicle on a public road. The process and conduct by North Wales Police in respect of its use of NAS is overseen by the Investigatory Powers Commissioners Office (IPCO)

The implementation of NAS is seen as a national improvement and there is standardisation in the way ANPR data is managed and processed. The processes are subject of audit in accordance with the [National standards for compliance and audit of law enforcement ANPR](#).

10.4 Purpose of Processing

The National Police Chiefs Council has in place an Automatic Number Plate Recognition (ANPR) Strategy for the period 2025 - 2028.

The National Strategic Vision and the Strategic Intent are to:

Strengthen and develop the existing fundamental capabilities that ANPR brings to protecting the public and reducing crime in relation to the following law enforcement activities;

- Operational Response – real-time response to ANPR matches relating to vehicles of interest,
 - Intelligence Development – using the value of ANPR data,
 - Investigations – using ANPR data to support investigations,
- and
- To ensure public confidence in the development, management and use of ANPR by law enforcement agencies taking account of privacy concerns, and maximising transparency.
 - To ensure ANPR data is managed responsibly and used proportionately for policing and law enforcement purposes only.
 - To maximise the benefits from the NAS as a cost-effective service to ensure consistent efficient and effective use of ANPR.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 16 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

10.4.1 Strategic Goals

The key goals over the period of the strategy are that the following will have been achieved:

- Police and LEA resources, processes and procedures are in place to realise the potential of ANPR in:
 - Providing consistent operational response to ANPR matches relating to vehicles of interest.
 - Providing complementary data analysis in intelligence, development, investigation and the management of demand
 - Improving proactive and targeted interventions.
 - Protecting the safety of road users and targeting high risk offending that can lead to road death.
- Police forces and LEAs adopt national training standards and guidance to professionalise their capability, ensuring full utilisation and optimisation of ANPR capability.
- Approved Professional Practice and operational capability guidance in ANPR is established within the College of Policing's (COPs) professional development framework and embedded where appropriate in national training.
- Elements of local technology infrastructure will have been decommissioned and costs will be reduced.
- NAS is providing cost effective functionality to support ANPR use in line with best practice.
- Consistent audit and monitoring of ANPR data and its use embedded within all police forces and LEAs.

In the absence of NAS, North Wales would have no capability to provide any meaningful ANPR support to law enforcement colleagues elsewhere in the United Kingdom and also its own ability to reassure and protect the local population would be significantly weakened. Without the ability to progress processes for the collection, management and submission of ANPR intelligence and evidence, obligations cannot be fulfilled in line with National ANPR Policing Standards (NASP).

ANPR is now part of a National system within which North Wales with its road links to the North West, South of Wales and to Republic of Ireland is an integral part.

The Home Office have driven this recent national business change which was commissioned by the National Police Chief Council (NPCC).

10.4.2 Organisational Context

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 17 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

The previous National ANPR Infrastructure (NAI) comprised of two core elements, a Back Office Facility (BOF) within North Wales and a single central NADC at Hendon (to be replaced by NASP) The previous BOF was decommissioned and replaced by an updated BOF , namely NDI /ViSCE which provides the connectivity to NAS and NADC (to be replaced by NASP) and links to the national infrastructure. An updated version of VISCE is being developed which will link to the NASP.

LEA's manage a network of cameras that record number plate sightings which are then transferred to the NAS and NADC (to be replaced by NASP) where the data is retained for 1 year.

Before NAS was implemented nationally between approximately 25 million and 35million ANPR reads are sent to the NADC daily. The NADC held approximately 20 billion records and the NAS has seen an increase since it was introduced with an average of 90 million reads a day.

In support of this data movement, as described above, the National ANPR infrastructure (NAI) is supported by [NASPLE](#) which specifies the minimum standards to be met by ANPR cameras. [NASPLE](#) also specifies the requirements to be met for the deployment of cameras within the NAI taking account of necessity, proportionality and privacy concerns.

[NASPLE](#) also sets out the responsibilities in the collection, management and use of ANPR data by forces.

10.4.3 Economic and Financial Environment

The police and other Law Enforcement Agencies continue to face significant challenges to reduce costs and increase efficiency. The National ANPR strategy recognises the importance of seeking efficiencies and cost reductions both operationally and in the technology infrastructure.

Initially the implementation of NAS provided an opportunity for forces to reduce infrastructure costs at a local level in terms of the technology used and in storage of data. However the inability of NAS to fulfil its obligations in terms of advanced analytical functionality has meant ongoing connectivity to the NADC (to be replaced by NASP) which has come at a cost to forces nationwide.

ANPR as an operational tool presents cost effective support to intelligence and investigations that can reduce the costs associated with other activities and shorten the time taken for an investigation to be concluded.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 18 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

NAS provides for appropriate access to national data that together with increased awareness of staff of the value of ANPR to their work will enable cost efficiencies to be achieved.

10.4.4 Operational Maturity

ANPR has been established to support core policing for operational response purposes for a considerable time although greater consistency in provision of monitoring and response is required.

During recent years there is evidence of the value of ANPR in improving national security, counter terrorism, intelligence led investigations for major and serious organised crime as well as more localised crime, all leading to the conviction of offenders. However, ANPR also provides reassurance and confidence in respect of Crime Prevention and Crime Reduction in our communities.

The maturity of the use of ANPR data varies across police forces due to knowledge and experience of staff and the limitations of access to data. This was particularly evident with previous arrangements for the management and use of data but is now improved with national access to NAS.

The strategy recognises the need for consistent and effective management of ANPR data supported by appropriate governance. NAS offers improved management functions within the ANPR application. Consistent management and audit requirements are defined within [NASPLE](#).

North Wales Police are fully dependant on and committed to NAS.

10.4.5 Privacy and Transparency

The proportionality in the deployment and use of ANPR by Law Enforcement Agencies and Police Forces and the impact on privacy is of continued interest. The standards for infrastructure development and for access and use of ANPR data within NASP have been developed with advice from the Information Commissioners Office in order to provide consistent and effective procedures and controls to support proportionate use of ANPR by forces.

NAS contains a large amount of data and it is recognised that transparency in the development of the NAI and the use of that data is important to maintain public confidence and support for Police ANPR.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 19 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

The Surveillance Camera Commissioner appointed under provisions of the Protection of Freedoms Act 2012 has published a [Code of Practice](#) that includes 12 principles that have been developed from a set of 14 principles previously published in respect of ANPR. Compliance with the principles within the Code by LEA assists in establishing and maintaining public confidence in the use of ANPR by Law Enforcement Agencies.

The strategy recognises the importance of respecting and addressing concerns regarding privacy and transparency. North Wales will consult appropriately regarding infrastructure development and provide appropriate information regarding the operation and use of ANPR, taking account of the need to safeguard the operational effectiveness of the NAI.

10.4.6 Capability Support to Law Enforcement Agencies

The Home Office strategic aim is to develop excellent practice in all LEA's as appropriate to their areas of operational responsibility.

The strategic aims in respect of real-time operational response to ANPR alarms relating to vehicles of interest, either through a control room or through self-deployment are:

- Police Forces and LEAs target improvement in their capacity to respond to alarms.
- Ensure that real-time monitoring and response is proportionate to the priority of the alarm.
- Ensure a consistent and sufficient response.
- Improve co-operation and co-ordination of response by police forces and LEAs.

The strategic aims in respect of intelligence development are to:

- Increase Police and LEA staff awareness of the opportunities provided to them by ANPR data.
- Ensure ANPR is embedded as a core intelligence product throughout law enforcement.
- Develop innovative and best practice for the use of ANPR in offender management and intelligence development to improve public safety.

The strategic aims in respect of investigation are to:

- Increase Police and LEA staff awareness of the opportunities provided to them by ANPR data.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 20 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

- Fully embed the understanding of ANPR capabilities and their use throughout the investigative process.
- Further develop and promulgate best practice in the use of ANPR data for surveillance and other forms of support to investigations

10.4.7 Infrastructure Development

The National ANPR Camera Strategic Group (NACSG) provides oversight of national infrastructure to:

- Ensure that current deployments are consistent between police forces and LEAs.
- Identify any potential duplication of capability arising as a consequence of integrating local systems into a single national system, with proposals for mitigation.
- Identify any gaps in infrastructure provision that may be mitigated by deployment of additional ANPR capability.

The criteria for the deployment of ANPR cameras has been reviewed and updated templates and guidance issued. Work is ongoing within the scope of this strategy to further establish national oversight of infrastructure via the NACSG.

Opportunities for collaboration between police forces, LEAs and other public and private sector operators of ANPR will be explored to rationalise the ANPR infrastructure and reduce the costs of establishing ANPR at locations where it is necessary and proportionate to do so. This will contribute to efficiency and take account of privacy concerns by reducing the number of cameras that are deployed at a location.

North Wales Police have aligned themselves with the majority of UK Police Forces in relation to the use and deployment of NAS.

11. Consultation Process

11.1 Internal Consultation.

Data Privacy considerations will have been addressed at the inception of ANPR in North Wales and/or at the introduction of new cameras or extension of its technical capability. Therefore, external stakeholders have been consulted previously and will likely see minimal or no change that will impact any community privacy concerns as a result of NAS.

ANPR is not a new concept for internal users and the basic process steps are still present even though NAS has been introduced. Though being part of a larger national group of users with a NAI, a single NASPLE guidance document has helped remove any deteriorating or poor local practices.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 21 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

NAS implementation therefore is designed to and will continue to force an improvement in process and data management by internal staff. This will further reassure the public over the use of ANPR thereby seeking support for its continued deployment. Therefore many, if not most data impact issues will have likely been addressed within the earlier stages of ANPR deployment in North Wales notwithstanding any recently implemented guidance and /or legislation.

New ANPR cameras that have been introduced in North Wales during 2022 and 2025 have been subject of consultation with Local Policing Teams at Police Inspector rank.

Local area Inspectors, whilst addressing local concerns have provided advice and support in respect of new ANPR cameras. This is to the extent of offering alternative sites for operational reasons and seeking to maximise the intelligence potential of ANPR.

The implementation of NAS within North Wales has been managed through a dedicated Project Board led by the Director of Intelligence who is the strategic lead for ANPR in North Wales.

The NAS Project Board structure included Corporate members in respect of Project Development and Management, ICT leads including ANPR team, Human Resources Training, Procurement and Information Standards and Compliance/Transaction Monitoring.

Those members who formed part of the initial consultation;

- The Director of Intelligence –ANPR Strategic lead /Project Executive provided overall governance of the Project and direction.
- The Project Manager provided a corporate approach to the NAS Project providing management and advice on the many issues within the life of the Project.
- The Business Manager provided advice on acquisition, cost effectiveness and procurement.
- The Data Protection Officer provided advice in respect of Data Protection issues including relevant National and Local Guidance and/or legislation

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 22 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

- The Information Security Assistant provided advice around the more technical data routes used and any security issues around property and /or organisations routing or storing the data.
- The Transaction Monitoring Team provided advice regarding the obtaining and use of data, ensuring compliance with the Data Protection and Surveillance Camera Commissioner Principles. This ongoing support provided by dip sampling NAS users as regards to necessity, proportionally, justification and record keeping.
- The Information Communication and Technology team (ICT) in liaison with Information Standards and Compliance ensuring that data routes and platforms are secure for processing ANPR data.
- It is the ANPR Managers responsibility to ensure that North Wales' data processes and data handling comply with [NASPLE](#).
- The ANPR team continue to provide advice from an operational perspective on any ANPR business related subject.
- The ANPR team will work closely with the Audit team to ensure Data Protection and Surveillance Commissioner Principles along with other legislative guidance /direction are complied with for deployment of ANPR within North Wales.
- The ANPR Team have provided Advanced level training to many NAS users making use of the Home Office Training packages available.
- Procurement provided advice on the acquisition and specification of any external products that are utilised to ensure North Wales ANPR data will get through to NAS securely.

The ANPR NAS Project Board no longer meet as a group but the ANPR and NAS are managed from within the North Wales Force Intelligence Bureau within Crime Services.

11.2 External Consultation

Self Assessment

The Office of Surveillance Commissioners have created a Self-Assessment Tool which poses questions to Police Forces regarding their considerations around privacy and in particular the 12 guiding principles within the Code of Practice.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 23 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

The Self-Assessment was first published in June 2018 on the North Wales Police public facing internet site. The latest Self-assessment was conducted January 2025.

National Public Survey

In 2020 Police Forces including North Wales took part in a public national ANPR survey. Whilst this was published by West Midlands Police statistical data is available from North Wales respondents.

Consultation with Local Councils

Ongoing consultation is taking place with Data Protection Officers across each of the local Councils seeking any responses particularly around the increasing size of the North Wales ANPR infrastructure.

Local Community awareness

As some of the former Welsh Government sites are identifiable by their structure some local residents are aware of their use and to date no objections have been forthcoming.

Opportunities for Consultation

North Wales Police will continue to ensure that the public are made aware of ANPR within the force area and its purpose in tackling crime. This would include marketing ANPR on the NWP website and other open source sites, plus where possible signage on the roads and leafleting etc.

12. Necessity and Proportionality

Legal Basis

The legal basis for ANPR is established by reference to the [Data Protection Act 2018](#), Common Law and is implicit from the [Protection of Freedoms Act 2012](#) that includes requirements for law enforcement use of ANPR to comply with the [Surveillance Camera Code of Practice](#).

Policing Purpose

The policing purposes outlined below establish a lawful basis for the processing of ANPR data in Common Law, in that the use of the data is both pressing and proportionate in the circumstances. ANPR technology is used daily by law enforcement and other agencies in the United Kingdom. It's uses falls within three primary categories:

- To identify vehicles of interest.
- To respond operationally to those vehicles
- Gather intelligence and further police capability to investigate crime and it is in this context that this deployment is considered.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 24 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

The management and use of ANPR must be in accordance with the provisions of [NASPLE](#) which provides detailed safeguards to ensure that the use is lawful and consistent with the requirements of legislation. The management and use of ANPR cameras deployed as a result of this assessment will be in compliance with those requirements.

The National NAS requirement:

- Improved Functionality
- To ensure public confidence in the development, management and use of ANPR by law enforcement agencies taking account of privacy concerns, and maximising transparency.
- To ensure a consistent approach in maximising the efficiency and effectiveness in the use of ANPR
- Accessibility of national data set
- To maximise the benefits from NAS as a cost effective service.

Local NAS/ViSCE requirement:

- To ensure public confidence in the development, management and use of ANPR by North Wales Police, taking account privacy concerns and maximising transparency.

The above will be achieved by:

- Ensuring Auditing standards are met as set by the Home Office.
- Full compliance with NASPLE.

There is no other way that North Wales Police would be able to achieve the information ANPR provides in order to help prevent and /or detect crime. It is important in retaining public confidence and support for ANPR. This is achieved by conducting regular reviews of our working practices which includes the methodology around our data collection, retention storage and deletion.

Local Auditor

NWP dedicated Auditor has responsibility to ensure operational compliance and report any areas for attention to the National Auditor.

The National Auditor holds forces to account and publishes quarterly force audit returns against National Standards. This process commenced in early 2022.

All audits must comply with the [National Standards for compliance and audit of Law Enforcement ANPR](#).

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 25 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

North Wales ANPR User considerations

In contemplating how North Wales Police deploy ANPR with a view to minimising infringements on privacy and reducing any collateral intrusion, there will be ongoing consideration from the outset of the data collection until such time that the potential risk has passed.

Individual users hold responsibility for compliance with NASPLE and are subject of auditing and transaction monitoring. However, they are supported by the ANPR team who are available during office hours and the i24 Team for out of hours support.

NAS users are aware of their requirement to comply with ECHR when using NAS.

When using NAS users must record their name, the incident they are dealing with and the reference number related to that task for each individual transaction. These details are required for auditing and checking for compliance against necessity, proportionality and justification. The ANPR Manager has day to day governance of ANPR and will be aware of any auditing concerns.

The Director of Intelligence as an Information Asset Owner has overall responsibility for procedure and process for ANPR within North Wales.

13. Collateral Intrusion

North Wales Police will attempt to minimise collateral intrusion at all stages. Whilst this is particularly evident when the ANPR data is first captured it will continue throughout the data handling process:

Examples include:

- The cameras do not record sound.
- The cameras only record still images.
- The cameras are set to focus only a small section of road around the vehicle.
- The cameras are configured in such a way as to screen out any areas which may affect privacy –for example a window of a house simply will not appear within image.
- The plate image only focusses on the plate patch area.
- Only specific data is captured: Time, date, location, overview vehicle images.
- Search time and date parameters are tightened and have to be justified to avoid over harvesting and subsequent release of data.
- Supervisory authority is required for extended searches over 90 days old.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 26 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

- The ANPR team provides a gatekeeper role for any requests and where necessary will reject unreasonable requests.
- Any data which does not relate to the subject is discarded appropriately.
- Data is only released from Intelligence Units to staff under government official marking and within intelligence reports which are risk assessed and applied with handling conditions.
- All data which is not preserved and not subject of PIRM or CPIA is deleted after 12 months.
- All ANPR users are trained and receive Data Protection training within the ANPR package.
- All North Wales Police and Staff receive separate Data Protection training as part of their role.
- All North Wales Police ANPR users and recipients of ANPR data are security vetted.
- All ANPR users and terminals are sited within secure police buildings or in cases of Agile Working (ie working from home) on secure encrypted devices.
- All data flow is regulated by the Government Protective Marking Scheme and intelligence graded and marked accordingly.

In most cases, persons captured on the ANPR system will be personally unaffected and have no concerns regarding the intrusion, as is the case with the majority of the population. The ANPR data is harvested and in the majority of cases will be appropriately disposed of, without ever having been accessed.

There are safeguards around the ANPR data collected on those individuals that have a propensity towards crime and this data will only be provided to officers and staff if the request is:

- Proportionate - in relation to the offence or incident being investigated.
- Lawful - ensuring compliance with legislation and being for a policing purpose.
- Appropriate - relevant to the advancement of the investigation.
- Necessary - the collection of ANPR data will not be the only means available of collecting data on an individual and so should only be used if it enhances the intelligence or evidence and the investigation should hold sufficient gravity to necessitate the use of ANPR data.
- Non Discriminatory - the data collected will have no relevance to a person's protected characteristics and is compliant with the Equality Plan.
- Justified - all data requests for investigations or intelligence must demonstrate that it is justified before the data will be provided.
- Audit - All data collected for investigations will be recorded and subject of independent audit.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 27 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

14. Social Pressing Need

The Governmental and National Policing objectives have changed over recent years. These changes are reflected in the varying cases and operations that North Wales Police are being asked to investigate.

There are a number of areas highlighted which include:

The Strategic Threat to National Security.

- The growth in acts of Extremism and Terrorism on the British mainland.
- Events in North Ireland (North Wales shares a border point with Ireland).
- The global increase in Cybercrime and the prevalence of cyber-attacks at all levels internationally, nationally and locally.
- Technological advances.

Serious and Organised Crime:

- Modern Slavery and Human Trafficking.
- Child Abuse cases within the United Kingdom.
- The increase in Organised Crime Groups and County Lines investigations. North Wales Police borders the North West and the A55 corridor provides ease of access to offenders.

Local Crime

- Increase in the number of reported offences with decreasing policing resources and budgets.

Community confidence and reassurance / crime prevention and reduction:

- Financial restraints coupled with the need for best value with limited resources.
- Increased volume of traffic on our roads.

North Wales Strategic Assessment

North Wales Police serves a population of approximately 687,800 people and covers an area of 6,300 square kilometres. The Strategic Assessment will affect all those people within that area and will include a transient population which increases in the summer season.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 28 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Given all police forces in the United Kingdom have ANPR capability, road users travelling between borders will potentially be subject of a breach of their privacy however, each force is bound by the same [NASPLE](#) and each will complete a strategic assessment.

The Strategic Assessment will detail why ANPR is required in meeting the Pressing Social Needs of the North Wales community.

15. Identify and assess risks

Describe source of risk and nature of potential assessment on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
The deployment of ANPR at a location is not proportionate	Remote	Minimal	Low
The decisions on deployment are inconsistent between LEA	Possible	Minimal	Low
Deployment of infrastructure presents duplication in the context of overall national infrastructure	Possible	Minimal	Low
Individuals not involved in criminal activity consider the new ANPR deployments as unjustified intrusion on their data and privacy.	Possible	Minimal	Low

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 29 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Action taken as a result of ANPR 'hits' from a camera may be seen as disproportionate, or the VRM may have been mis-read.	Possible	Minimal	Low
Inappropriate disclosure of data	Possible	Significant	Medium
Excessive data is collected	Remote	Minimal	Low
Data is retained longer than necessary	Remote	Significant	Low
Deployment will be considered disproportionate and subject to complaint to ICO.	Possible	Minimal	Low
ICO may determine that deployment is inappropriate leading to sanctions.	Remote	Significant	Low

16. Identify measures to reduce risk

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes
The deployment of ANPR at a location is not proportionate	Assessment of 'Pressing Need' supported by a detailed strategic	Risk reduced	Low	Yes - A robust assessment process for infrastructure development provides a

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 30 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

	assessment, decisions taken following consultation and consideration of all issues.			proportionate response to the aims of the project taking account of any privacy concerns
The decisions on deployment are inconsistent between LEA	Consultation with and oversight by the National ANPR lead for ANPR	Risk reduced	Low	Yes
Deployment of infrastructure presents duplication in the context of overall national infrastructure	Consultation with and oversight by the National ANPR lead for ANPR	Risk reduced	Low	Yes
Individuals not involved in criminal activity consider the new ANPR deployments as unjustified intrusion on their data and privacy.	Transparency in regard to ANPR with provision of information concerning why it is needed, how it is used provide via Internet sites, written communication and through appropriate signage. Access controls in place in accordance with NASPLE	Risk reduced	Low	Yes - Increased awareness of how ANPR is used and the controls in place to prevent misuse will reduce concerns.
Action taken as a result of ANPR 'hits' from a camera may be seen as disproportionate, or the VRM may have been mis-read.	Management controls in place to ensure use is in accordance with NASPLE . Robust process for managing lists of vehicles of interest to ensure that data for circulated vehicles remains accurate and relevant.	Risk reduced	Low	Yes - Efficient business process will reduce the likelihood of inaccurate data and compliance with policy on use will ensure that use is proportionate.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 31 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

	Ensure compliance with NASPLE for system performance.			
Inappropriate disclosure of data	Data is only shared and accessed in accordance with NASPLE . Provisions for monitoring and audit of data access and use in place.	Risk reduced	Low	Yes - Compliance with business rules provides safeguards to prevent misuse and enable the benefits from the development to be realised
Excessive data is collected	ANPR is only deployed where a pressing need has been identified. The continued requirement will be reviewed in accordance with NASPLE . Retention and disposal of data is in accordance with NASPLE .	Risk eliminated	None	Yes - Compliance with NASPLE ensures that data is collected and managed in accordance with agreed national standards. This should be measured against the success criteria identified at the outset, pressing need should also be kept under review
Data is retained longer than necessary	Compliance with NASPLE regarding retention and disposal of data	Risk eliminated	None	Yes - Compliance with NASPLE ensures that data is collected and managed in accordance with agreed national standards.
Deployment will be considered disproportionate and subject to complaint to ICO.	Compliance with national guidance for the development of ANPR infrastructure. Decisions taken following strategic assessment taking account of identified privacy concerns identified through timely consultations	Risk accepted	Low	Yes - Decisions regarding deployment are taken following proper assessment, nonetheless it is recognised that some may disagree with the decisions and the opportunity for review by the ICO is an essential safeguard.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 32 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

	with appropriate groups and individuals.			
ICO may determine that deployment is inappropriate leading to sanctions.	Compliance with national guidance for the development of ANPR infrastructure. Decisions taken following strategic assessment taking account of identified privacy concerns identified through timely consultations with appropriate groups and individuals.	Risk reduced	Low	Yes - A robust development and review process reduces the likelihood of ICO review concluding that the deployment of infrastructure at a location is inappropriate.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 33 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

17. Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	DI W Garton	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	DI W Garton	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Head of Information Assurance	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The collection and processing of data is proportionate and necessary. Risks concerning personal data have been identified and suitably assessed and accepted where required. The force adheres to NASPLE and data protection legislation in respect of access, management and the use of ANPR data, including audit provisions. The national data is hosted in secure data centres with appropriate physical security. National data is protected by technical security controls. Access to data is restricted through technical measures such that attempts to access from unauthorised networks are rejected. Data being transferred to or from national systems is protected through appropriate cryptographic controls to protect and encrypt data in transit. NWP have a local DPA in place with NDI (expiry October 2026) who processes the data on NWPs behalf in order to transfer to NAS.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 34 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Comments: **ENTRY REQUIRED**		
Consultation responses reviewed by:	**ENTRY REQUIRED**	If your decision departs from individuals' views, you must explain your reasons
Comments: **ENTRY REQUIRED**		
This DPIA will kept under review by:	**ENTRY REQUIRED**	The DPO should also review ongoing compliance with DPIA

Appendix i

North Wales Static ANPR Camera Capability

Note* For the purposes of this DPIA and to prevent disclosure of sensitive ANPR camera site locations, all cameras are identified by their North Wales Police asset number which is assigned to each individual camera.

Furthermore ANPR cameras have been grouped together into clusters within the wider geographical areas of North Wales to assist with:

- Identifying camera sites within that specified geographical area.
- Where necessary, ensuring that a '*pressing need*' for ANPR at a location can be detailed specifically and individually as opposed to generically for all cameras.
- Detail any demographic /populous/traffic volume/crime trend concerns for specific areas.

EASTERN	
Wrexham Town /Rural	Wrexham has a resident population of almost 136,000. The proximity to the English border and the major urban hubs of Liverpool and Manchester creates significant risks from travelling

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 35 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

	offenders who seek to exploit vulnerabilities within communities across North Wales. These travelling criminals will likely to be unknown to local law enforcement and partner agencies and will bring a level of sophistication to their offending model with a heightened threat through the use of serious violence, weapons and exploitation. Historically, analysis shows that 1 in 5 serious violence offences are linked directly to drugs disputes or drug supply criminality, with debts being the typical driver for the use of violence. Gangs operating the County Lines drug supply model continue to exploit children and vulnerable adults to both move and store their commodities, through the use of coercion, intimidation, violence and weapons. The groups that consistently pose the highest risk in Flintshire and Wrexham are those who are targeting the most vulnerable people in our society, this can be children who are coerced into criminal or sexual exploitation or drug users and people with mental health issues who are sought out to use their homes as a base for drug supply. The continued targeting of youths for child criminal exploitation (CCE) remains a very concerning trend. It can take many forms, but in North Wales CCE is most commonly associated with the County Lines drug supply model. Victims typically have existing vulnerabilities which make them particularly susceptible to being targeted. They are likely to come from a chaotic home environment, be exposed to substance abuse and domestic violence from an early age, will regularly go missing or be truant from school and reside in neighbourhoods with high crime rates. Areas where organised crime is prevalent often have common characteristics of high levels of deprivation, child poverty, crime rates, unemployment, benefit dependency and low levels of household income. Organised Crime Groups will have detailed knowledge of vulnerabilities in local areas and seek opportunities to exploit vulnerable individuals. Analysis of North Wales again shows that areas considered most vulnerable generate a disproportionately high amount of calls to emergency services for criminal offences, antisocial behaviour and safeguarding concerns. These areas have significantly higher than average levels of social housing, repeat absenteeism and benefit claimants. This along with substance dependency, mental health concerns and delinquent peer influences combine to produce favourable circumstances for SOC
--	--

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 36 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

	networks to exploit, recruit or coerce their victims in order to further their criminality. Serious / Organised Acquisitive Crime (SOAC) offences are often committed by criminals who are well prepared and will travel across police force areas to target specific locations chosen due to a particular commodity or vulnerability. Offences in North Wales are often linked to cross-border series and the proximity of Flintshire and Wrexham to the English border means there is a concentration of serious acquisitive crime in the authorities, particularly car key burglaries. HMP Berwyn is within the Wrexham Borough. In December 2019 remand prisoners were accepted into HMP Berwyn, pushing the prison population to approximately 1,700. This increase is likely contributed to an increase in 'Throw overs' of contraband. Serious Organised Crime in prisons is highly lucrative with mobile phones continuing to be an enabler. Prisons are becoming increasingly aware of OCG members housed within their establishments. HMP Berwyn has the highest number of inmates of all prison establishments in the North West of England and North Wales. In late 2021 a consultation questionnaire was sent to North Wales District Police Inspectors ahead of this DPIA. The Wrexham District Inspector responded in full explaining the value of ANPR in the Wrexham Town and Rural areas highlighting recent County Lines successes quoting individual operations. The cameras within the general Wrexham area are grouped for the reasons provided above. Within this group are camera sites which include: • Wrexham town including ANPR coverage around the Industrial estates and Prison areas • Wrexham Rural-These cameras provide ANPR coverage for many of the feeder routes into and out of the Wrexham town centre area in all compass directions Further information in relation to each individual site within this group is set out below:
--	--

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 37 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Location Name Redacted	nwp28903	Single camera site capturing vehicles to the north east of Wrexham.
Location Name Redacted	nwp31591 nwp34581	This site south west of Wrexham in the Llangollen, Chirk area includes previously owned WG cameras. Two cameras at this location capture vehicles travelling between local towns.
Location Name Redacted	nwpC0001 nwpC0002 nwpC0003	Several town centre sites in Wrexham located on class B roads. These sites are relatively new having been commissioned in 2017 in response to a local building project.
Location Name Redacted	nwp28902	Single camera site capturing vehicles travelling to the west of Wrexham.
Location Name Redacted	nwp28905	Single camera site capturing vehicles travelling to the east of Wrexham.
Location Name Redacted	nwp28906 C0040	Single camera site capturing vehicles travelling in the areas to the south of Wrexham.
Location Name Redacted	nwp28904	Single camera site capturing vehicles travelling in the areas to the south west of Wrexham.
Location Name Redacted	CO017 CO018	Several camera sites previously owned by WG located around Wrexham town area commissioned in 2021. Funded by Safer Communities identified as result of local concerns around increasing crime in and around the Wrexham area.
Wrexham area and English Border routes		North Wales Police area shares borders with West Mercia, Cheshire and Dyfed Powys. The sites include some ANPR coverage for the border routes with Cheshire and Shropshire. This camera group features ANPR camera installations predominately to the North, the East and the South of Wrexham. Whilst the traffic flow between the North West and the North Wales coastal town areas brings an increase of criminality to those areas. Similarly the towns and rural areas to the south of the force area see travelling criminals accessing the heart of North Wales to and from the Midlands and mid Wales. Wrexham County whilst not on any coastal area is still exposed to high levels of criminality.
Location Name Redacted	nwp31590 nwp34580 nwp31568	This site north of Wrexham comprising a number of cameras capturing traffic on border routes between North Wales and England. Site includes previously owned WG cameras.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 38 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

	nwp28902	
Location Name Redacted	nwp34580	This site North of Wrexham identified at recent Strategic Review and was commissioned into service in 2022.
Location Name Redacted	nwp31568	Single camera site capturing vehicles travelling in the south of Wrexham capturing vehicles along border routes with England.
Location Name Redacted	nwp31589	This site includes previously owned WG cameras. Several cameras capturing vehicles travelling on routes south of Wrexham around Gobowen, Chirk and Llangollen which provide access into the heart of North Wales. Camera site moved a short distance in 2018 at request of ANPR team in response to several attacks in succession where the cameras were damaged /stolen by persons unknown.
Flintshire East		Flintshire has a resident population of approximately 156,000. The Deeside area and the A55 Gateway to North Wales is the primary route for criminality from the North West. At this point in Deeside there are also opportunities to take the coastal A548 route stretching as far west as Pensarn in the county of Conwy where it rejoins to the A55 expressway and beyond, providing access to the western area of the force. This group includes a number of rural camera ANPR sites and provides ANPR coverage predominantly to the North Flintshire area.
Location Name Redacted	nwp31582 nwp34575 nwp34576 nwp31570 nwp31573	The Flintshire sites include arterial routes into North Wales and feeder/local routes between Chester and the North East of North Wales. This area incorporates two former WG sites.
Location Name Redacted	nwp34607 nwp34608 nwp34609 nwp34610 nwp34611 nwp34612 C0039 nwp31590 nwp34580	This North East area of Flintshire incorporates several sites including A Class Roads predominately capturing vehicles entering and leaving North Wales. A camera set in this area captures vehicles making use of the main coastal route of North Wales.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 39 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Location Name Redacted	nwp34615 nwp34616	This area of Flintshire incorporates several sites including arterial routes into North Wales and local road network between Hawarden, Broughton Mold and Ewloe.
Location Name Redacted	nwp34614	Single Flintshire camera site in the Sychdyn, Buckley, Mold area capturing vehicles travelling between the North West and into the north east corner of Wales.
Location Name Redacted	nwp31583 nwp34578	This Flintshire site between Mold and Connahs Quay includes previously owned WG cameras capturing vehicles around on main arterial routes into North east area of Wales.
Location Name Redacted	nwp31572 nwp31584 nwp34582	Single Flintshire camera site between Mold , Buckley and Northop capturing vehicles travelling on local routes between towns in North East Wales.
Flintshire West		Flintshire West ANPR overage includes North Wales coastal routes, the A55 expressway as it passes through the county and a number of inland camera sites. Along with serving the towns in the Flintshire area the ANPR coverage includes capturing vehicles traveling further westbound into North Wales. This area of road network is described by the local Policing Inspector as a ' <i>conduit for OCG drug business</i> '.
Location Name Redacted	nwp31571	Single Flintshire camera site capturing vehicles travelling in the area north east of the A55 Expressway in Flintshire.
Location Name Redacted	nwp28890 C0038	Single camera site capturing vehicles travelling in the North Wales coastal area around Holywell and Mostyn.
Location Name Redacted	nwp28889	Single Flintshire camera site between Flint and Deeside capturing vehicles travelling in the North East coastal area of Wales.
CENTRAL		

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 40 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Conwy West and Conwy Valley	Conwy has a residential population of 117,900. This area of North Wales has a number of beauty spots and sees a high influx of tourists during the late spring and summer. In 2020 a Vulnerable Localities Index of 6 sociodemographic factors has identified localities that are likely to require prioritised attention from public agencies. These vulnerable localities generate a disproportionately high amount of demand for law enforcement and partner agencies and there are significant overlaps of seemingly unrelated incidents, from low level delinquency to serious <i>organised crime, that occur within concentrated areas of our communities.</i> In Conwy these vulnerable localities are in Llandudno, Colwyn Bay and Abergele. Signs of County Lines activity in respect of drug dealing may also include the home addresses of vulnerable individuals being taken over, or ‘cuckooed’, by unknown people. ‘Cuckooing’ is the term used to describe the practise where drug dealers take over the property of a vulnerable person and use it as a place from which to run their business. Vulnerable tenants will be targeted, potentially as a result of substance abuse, mental health issues, or loneliness. Drug dealers will target these individuals and offer them free drugs, sexual favours, or their company for use of their property to sell drugs. As the victims of cuckooing are vulnerable, they are often fearful of going to the police and worry that they will be incriminated in the criminality. It is assessed by NWROCU that regionally cuckooing is the dominant method of obtaining access to suitable premises in order to store weapons, drugs and trafficked children and the practice is particularly prevalent within the North Wales force area. In 2020 the oldest identified victim was 89 years of age at an address in Llandudno. Hotspots for identified cuckooed addresses are consistent with known County Lines’ activity in Conwy and Denbighshire and have been the main areas being Llandudno, Colwyn Bay and Rhyl.
------------------------------------	--

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 41 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

		The cameras in this group contain both dual carriageway coverage and also single lane traffic in rural locations.
Location Name Redacted	nwp31595 nwp34592	This site includes previously owned WG cameras covering traffic routes between Blaenau Ffestioniog, Dolwyddellan, Capel Curig, Llanwrst and Cerrigydrudion.
Location Name Redacted	nwp31593 nwp34591	This site includes previously owned WG cameras covering traffic routes around Llandudno Junction, Llanwrst, Glan Conwy and Eglwysbach.
Location Name Redacted	nwp31592 nwp34590	Single camera site capturing vehicles travelling in the Conwy Valley area around Llanwrst and Betws y Coed. This site includes previously owned WG cameras.
Location Name Redacted	nwp31587 nwp34588 nwp34589 nwp34705	This site includes previously owned WG cameras covering routes between Llandudno, Llandudno Junction, Colwyn Bay, Glan Conwy and Penmaenamwr.
Location Name Redacted	CO025 CO026	This site was active until 2019 when it was decommissioned due to concerns over safety at its previous location. The new site commissioned in 2021 includes previously owned WG cameras and covers the areas around Bangor, Penmaenmawr, Llanfairfechan and Llandudno Junction.
Denbighshire Coastal		Denbighshire has a residential population of 95,700. Crime rates in Denbighshire are the joint highest by head of population in North Wales with 94 offences per 1000 residents a year. This is largely driven by high volumes of acquisitive crime and violent offences in the county. Denbighshire Coastal and in particular Rhyl, has the highest number of active County Line groups in North Wales. The majority of these OCGs are based in the large urban areas of Northern England, especially Liverpool. The use of the road system is the primary means by which these groups transport themselves and controlled drugs in to the area. Denbighshire Coastal is also one of the biggest tourist destinations in the country. Over the period between May

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 42 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

		and September the transient population increases by up to 50,000 each week. Historically all crime types increase over this period and the use of ANPR is vital in monitoring movements of offenders into and out of the area. This group of Denbighshire Coastal cameras includes ANPR coverage for roads within rural locations and also dual carriageway traffic.
Location Name Redacted	nwp31586 nwp34586 nwp34587	This site in the Abergele /Pensarn area includes previously owned WG cameras.
Location Name Redacted	nwp28891 CO016	Several camera sites in the Prestatyn area provide coverage in and around Prestatyn and the routes to and from Rhyl and the east of North Wales.
Location Name Redacted	nwp31575 nwp31576 nwp31579 CO013 CO014 CO015	Several camera sites in the Rhyl costal area provide coverage in and around Rhyl/Prestatyn and the routes to and from Rhyl. Several sites were funded by Safer Communities funding and were commissioned in 2021.
Location Name Redacted	nwp28901	Single camera site capturing vehicles travelling in the Towyn/Pensarn/Kinmel Bay area areas.
Location Name Redacted	CO027 CO028	ANPR Cameras commissioned in 2021 by WG. This area south of Denbigh identified by ANPR Team in consultation with local officers as being an area of North Wales with limited ANPR coverage in the heart of rural North Wales.
Location Name Redacted	nwp34617	Single camera site captures vehicles between Llangollen, Bala, Ruthin and Cerrigydrudion.
Denbighshire Rural		This group of cameras includes ANPR coverage for roads within rural locations and also dual carriageway traffic. The camera locations in this group cover access to the Denbighshire Coastal area, which is one of the biggest tourist destinations in the country. Over the period between May and September the transient population increases by up to 50,000 each week.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 43 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Location Name Redacted	nwp31585 nwp34583	This site south of Rhuddlan includes previously owned WG cameras situated in inland in the Denbighshire area.
Location Name Redacted	nwp34584 nwp34585	This site includes previously owned WG cameras. Several separate sites covering routes between St Asaph, Caerwys and Halkyn.
WESTERN		
Gwynedd North		Gwynedd has a residential population of almost 124,000. A Vulnerable Localities Index of 6 sociodemographic factors has identified localities that are likely to require prioritised attention from public agencies. These vulnerable localities generate a disproportionately high amount of demand for law enforcement and partner agencies and there are significant overlaps of seemingly unrelated incidents, from low level delinquency to serious organised crime, that occur within concentrated areas of our communities. In Gwynedd, the vulnerable localities are located in Caernarfon, Bangor and Bethesda. The Gwynedd North group of cameras includes: Rural locations, town locations, dual carriageway cameras and also detail of a proposed site yet to be commissioned given construction works on that stretch of road.
Location Name Redacted	nwp31588 nwp34593 nwp31581	This site includes previously owned WG cameras and includes several camera sites capturing vehicles travelling in the Bangor area.
Location Name Redacted	CO032	Single camera site capturing vehicles travelling in the Caernarfon area. This site includes previously owned WG cameras.
Location Name Redacted	nwp31594 nwp34594	Single camera site capturing vehicles travelling in a rural area to the south of Bangor. This site includes previously owned WG cameras.
Location Name Redacted	nwp31601 nwp31601 nwp34600	Single camera site capturing vehicles travelling to the west of Corwen and east of Trawsfynydd. This site includes previously owned WG cameras.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 44 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Location Name Redacted	nwp31780 nwp34598	This site captures vehicles in the Penygroes, Llanwnda and Caernafon areas and includes previously owned WG cameras.
Anglesey		Anglesey has a residential population of almost 70,200. The A55 dual carriageway stretches from the Menai Bridge town area to Holyhead and takes vehicles to Holyhead Port and from there travelers and their vehicles can go to Ireland via the ferry links. The island of Anglesey is accessible from the East via two bridges with one of this providing access along the A55 carriageway. Anglesey with its coastal areas much like many other areas of North Wales has a high density of tourists over the summer season. ANPR on Anglesey provides support for Wylfa nuclear power station (and still potentially Wylfa B), RAF Valley and Armed Forces training centre (Indefatigable). The current UK threat level is SEVERE and so it is essential that these locations have that ANPR capability.
Location Name Redacted	nwp34621 C0023 C0024	Camera site capturing vehicles travelling around the south east Anglesey area.
Location Name Redacted	CO019	Single camera site capturing vehicles travelling in the mid Anglesey area commissioned in 2021 and includes previously owned WG cameras.
Location Name Redacted	nwp34620 nwp34619	Single camera site capturing vehicles travelling in the south east Anglesey area.
Location Name Redacted	nwpC0004 nwpC0005 nwpC0006 nwpC0007 nwpC0008 nwpC0009 nwpC0010 nwpC0011	A number of camera sets found around the Holyhead /Port area of strategic importance to Counter Terrorism with its ferry links to Ireland. It is still one of the busiest UK Ports and is the main gateway in/out of UK/Ireland with approximately 2 million customers in 2020. The Holyhead Ferry /Road links are an easy passage for travelling criminals between Europe and Ireland as well as the UK. The Port has been used for many crime types

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 45 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

		including cases of exportation of stolen goods, people trafficking and illegal immigration.
Gwynedd South		Predominantly rural ANPR locations in the centre of North Wales in the Snowdonia National Park area with no coastal routes. Gwynedd South suffers all types of crime including Burglary, Theft of caravans, high value motor vehicles and farming equipment. The area is accessible from Dyfed Powys and from the English midlands areas bring a transient tourist population particularly so during the summer months.
Location Name Redacted	nwp31600 nwp34599	This camera set(s) comprising several camera sites including previously owned WG cameras.
Location Name Redacted	nwp34596 nwp34595 nwp31596 nwp31780 nwp34598	This camera set(s) comprising several camera sites including previously owned WG cameras provides links to the north, the east and mid Wales.
Location Name Redacted	CO022	This camera set includes previously owned WG cameras commissioned in 2021 provides coverage for the general area around Dolgellau.
Location Name Redacted	CO029 CO030 CO031 nwp31574 nwp31598 nwp31601 nwp34600	This camera set(s) comprising several camera sites including previously owned WG cameras commissioned in 2021. The site has road links toward Porthmadog to the west and south to Dyfed Powys. Also covering routes to the north and east of Wales.
Gwynedd West and Llyn Peninsula		High transient population in the summer months affects this area with tourism from the West Midlands and North West.
Location Name Redacted	nwp31598 nwp31574	This camera set(s) comprising several camera sites covering north, east and westbound traffic on the Llyn Peninsula.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 46 of 46	

OFFICIAL

Automatic Number Plate Recognition (ANPR) Data Protection Impact Assessment

Location Name Redacted	nwp31597 nwp34597	These camera set(s) comprising several cameras captures vehicles using the Llyn Peninsula.

Appendix

North Wales Mobile ANPR Capability

The North Wales Police Fleet has a number of vehicles with ANPR equipment therein and these are managed by North Wales Police. There are also a number of vehicles within the Firearms Alliance collaboration managed by Cheshire Police but are financially supported by both forces. These Alliance vehicles are sited in the Cheshire area and feature on the North West Strategic Roads vehicle groups on NAS.

Note * The Roads Crime Unit vehicles are all named and identifiable according to their call sign. However the Local Policing Vehicles when introduced into service many years ago were assigned to physical police stations across the force area. In the following years vehicles have been commissioned in and out of service, Force restructuring has subsequently taken place and most of the vehicles and their stations have been re assigned. Therefore for the purposes of this DPIA the vehicles are identified by the Force/Unit/Code (FUC) which is assigned to all cameras feeding into NAS.

Draft Version 0.1	Controlled Document	Date: 05/03/25
	AUTHORISED COPIES ONLY	
Document Reference ANPR-DOC-07	OFFICIAL	Authorised by: DI...
	Page 47 of 46	



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

BODY WORN VIDEO POLICY

POLICY

Governance:	Senior Leadership Team		
Document Type:	Policy		
Policy Owner:	Chief Information Officer		
Department:	Crime Services		
Policy Writer:	Chief Information Officer		
Policy Number:	144	Version:	1.9
Effective Date:	30/09/2024		
Recommended Review Date:	30/09/2025		

CHANGE HISTORY				
Version No	Date	Author	Changes	Ratification
1.2		... with support from the Force Governance and Policy Team	Transferred to new corporate template and new policy standards applied	
1.3		... with support from the Force Governance and Policy Team	Minor amendment following consultation	
1.4		...	Remove reference to mandated use of BWV in domestic incidents.	
1.5		...	Amendments to include reference to personal issue and pool issues BWV. Also transferred to new corporate template following review as part of policy threshold introduction	
1.6		...	Para 5.14 added - Capturing Images of CCTV / Phone Footage on Body Worn Video Cameras	
1.7	17/08/22	...	Para 5.10 added – Use of BWV in mental health units.	
1.8	TBC	...	Policy review to incorporate 2022 NPCC Guidance.	
1.9	30/09/24	...	Policy amended to reflect best practice in use of BWV at domestic abuse incidents.	

CONTENTS

1. WHY IS THIS POLICY REQUIRED?	3
2. WHO SHOULD USE THIS POLICY?	3
3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?	3
4. ROLES AND RESPONSIBILITIES	8
4.1 BWV Users.....	8
4.2 Local Supervisors /Custodian.....	8
4.3 Systems Administrator / Information Asset Owner.....	8
5. THE PROCESS	8
5.1 Requesting and Issuing a Body Worn Video Device	8
5.2 Recording an Incident.....	9
5.3 Objections to Recordings.....	10
5.4 Public Requests to Record	11
5.5 Collateral Intrusion	11
5.6 Private Dwellings.....	11
5.7 Forced Entry into Premises as part of a Warrant	12
5.8 Crime Scenes.....	12
5.9 Use of BWV in Reports of Rape or Serious Sexual Assault.....	13

5.9.1	Anonymity.....	13
5.9.2	Explicit and Informed Consent.....	13
5.10	Use of BWV in Mental Health Units.....	14
5.11	Concluding a Recording	14
5.12	Post Incident	14
5.12.1	What is Post Incident?	14
5.12.2	Initial Action.....	14
5.13	Stop & Search	16
5.14	Selective Capture and Book Marking.....	17
5.14.1	Selective Capture	17
5.14.2	Book Marking.....	17
5.15	Capturing Images of CCTV / Phone Footage on Body Worn Video Cameras.....	18
5.16	Witness First Accounts.....	18
5.17	Recording of Interviews	19
5.18	Witness Identification.....	19
5.19	Uploading, File References and Exhibits.....	19
5.19.1	Evidential Footage	22
5.19.2	Burning evidential footage to DVD (working copy) for submission to AJD (and then CPS)...	22
5.20	Requests for Editing or Producing CD/DVD's - Imaging Unit - Crime Services.....	23
5.21	Officers Viewing Footage Prior to Making a Statement.....	23
5.22	Use by Professional Standards Department (PSD).....	23
5.23	Provision of Data to Outside Organisations	24
5.24	Body Worn Video in Public Order Deployments	24
5.25	Mutual Aid.....	25
5.26	Retention & Disposal	25
5.26.1	Retention and Legislation	25
5.26.2	Disposal.....	25
6.	DECLARATION & LEGALITIES.....	25

Yellow Highlighted sections are exempt from publication: S31 of the Freedom of Information Act 2000 in relation to Law Enforcement.

1. WHY IS THIS POLICY REQUIRED?

This policy will

- 1.1** Ensure officers make best use of Body Worn Video (BWV) technology to ensure a safer North Wales by preventing crime and disorder and where appropriate gathering evidence to support bringing offenders to justice. BWV will assist users in achieving this by:-
 - Reassuring the public and improve trust and confidence.
 - Increasing and improving intelligence gathered.
 - Assisting Criminal Justice partner agencies in delivering best evidence.
 - Reducing Officer case build time and court appearances.
 - Ensuring BWV is used in compliance with relevant legislation.
 - Increasing control of digital evidence as a crime exhibit.
- 1.2** Enable officers to comply with legislation and guidance to capture best evidence for use in court proceedings.

2. WHO SHOULD USE THIS POLICY?

- 2.1** This policy should be used by all police officers and police staff, including the extended police family and those working voluntarily or under contract to North Wales Police.
- 2.2** This policy particularly applies to those officers and staff employed within business areas, that are main users of BWV technology and its evidential product.
- 2.3** This policy includes :-
 - Clear direction for those trained in the use of BWV equipment including how to use the device, the retention of footage and how to share footage.
 - Clear direction on the management of data obtained via BWV.

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

- 3.1** BWV is an overt method by which officers can obtain and secure best evidence at the scene of incidents and crimes.
- 3.2** BWV significantly enhances evidence gathering opportunities and when available should be used in all appropriate circumstances. To enable this, all users must be aware of their responsibilities in relation to its deployment and retention to safeguard users and the integrity of the digital product.
- 3.3** When used effectively BWV can promote public reassurance, capture best evidence, modify behaviour, prevent harm and deter people from committing crime and anti-social behaviour. Recordings provide independent evidence that improve the quality of prosecution material and may reduce the reliance on victim evidence, particularly those who may be vulnerable or reluctant to attend court.

- 3.4** BWV can also impact on the professionalism of the service and assist in the continual development of our staff. Officers, trainers and supervisors can utilise the equipment to review and improve interactions and interventions.

All images recorded are the property of North Wales Police and must be retained in accordance with force procedures and the National Police Chiefs' Council (NPCC) Practice on Police Use of Digital Images. Images are recorded and retained for policing purposes and must not be shown or given to unauthorised persons.

3.5 The Equipment

The BWV equipment is a body-mounted camera with a built in microphone. The camera stores digital files, which, once recorded, cannot be deleted or amended by the operator. Each digital file carries a unique identifier and is time and date stamped throughout. The dedicated software, Digital Evidence Management System (DEMS) manages the downloading and storage of the digital files. This provides a full audit trail ensuring evidential continuity is maintained.

BWV is deployed in NWP on both a Personal and Pool issue basis.

- **Personal Issue** – BWV devices are marked with the user's collar number, and must only be used by the asset owner. These devices will be docked in clearly labelled docking stations.

Pool Issue – BWV devices are available for some users and can be "booked-out" each time. These pool issue devices will be docked in clearly labelled docking stations "Pool BWV" and can be booked-out by a user who does not have a personal issue device. After consultation with their Custodian these devices can also be used by Personal Issue Officers who have experienced a fault with their own device and where no spare is available.

3.6 Key Principles for the Overt Use of BWV

The Home Office and the College of Policing (CoP) produced [guidance](#) with seven key principles for BWV.

Principle 1	The use of body-worn video by police is lawful. Common law authorises BWV use in the lawful execution of their duties to prevent and detect crime.
Principle 2	Data is processed and managed in line with Home Office Code of Practice on the Management of Police Information (2005), College of Policing (2013) APP on Information Management and the principles of the Data Protection Act (DPA) (2018). Data retention, review and disposal must be in line with relevant legislation and current guidance. Forces must be able to ensure the integrity of data throughout the process and have due regard for the Home Office (2013) Surveillance Camera Code of Practice .
Principle 3	The normal use of body-worn video will be overt.

	Chief Officers must ensure that the capabilities of BWV equipment are clear to the public. This includes capturing audio as well as visual imagery. BWV may be used in covert policing subject to the relevant authorities.
Principle 4	The operational use of body-worn video must be proportionate, legitimate, and necessary. Complying with the Human Rights Act 1998, Data Protection Act 2018 and the Surveillance Camera Code of Practice will ensure the use of BWV is always proportionate, legitimate and necessary. Continuous, non-specific recording is <u>NOT</u> permitted.
Principle 5	Use of body-worn video will be incident specific. Officers will use common sense and sound judgement when using body-worn video, in support of the principles of best evidence. The use of Body Worn Video is mandatory for attendance at all Domestic Abuse/Violence incidents. Any decision not to use BWV should be recorded. Officers are required to justify their use of BWV. There should be a tendency towards capturing audio/visual evidence when deciding whether to record. Nevertheless there are several limitations.
Principle 6	Body-worn video supports, but does not replace, conventional forms of evidence gathering (i.e., written statements and Police and Criminal Evidence Act 1984 (PACE) interviews). Officers will continue to follow current practices for achieving best evidence.
Principle 7	Forces will consult locally with their communities on the use of body-worn video. Engagement will be proportionate to the local level of impact, which will be influenced by a force's decision to deploy BWV. Forces should carry out consultation to show due regard for the Public Sector Equality Duty and the Surveillance Camera Code of Practice. Consultation is also required for completing a Data Protection Impact Assessment and to comply with fair processing regulations in accordance with the DPA.

3.7 Training

All users must complete the North Wales Police on-line learning package. The training and additional guidance on DEMS and a Frequently Asked Questions document can be accessed through the intranet. The E-Learning package can be completed individually or as a team led by a Supervisor.

All student officers receive an input on the use of BWV as part of their classroom based training. Once the student officers are sent their BWV devices the BWV Supervisor shares the BWG guidance with them via email.

Local (station level) BWV champions are nominated to guide and assist users should they have any questions about the device or its use.

Only officers who have completed the necessary training will be issued the equipment.

3.8 When to Use BWV – ([Principle 5](#))

BWV overt recording can be used across a wide range of policing operations and incidents. Its use is inappropriate in only a few situations. Users must use their professional judgment with regard to recording.

The camera should be switched on when footage might support 'professional observation' or would corroborate what would be written in a Police issue pocket notebook.

There should be a tendency towards capturing BWV evidence when deciding whether to record. Nevertheless there are several limitations.

Users must activate BWV to record events in the following specific circumstances <u>Unless</u> there is a legal or operational reason not to do so which you must record in your Pocket Note Book (PNB).
• Attending premises in order to affect an arrest.
• The use of Body Worn Video is mandatory for attendance at all Domestic Abuse/Violence incidents.
• Prior to entering any land, premises, vehicle, vessel or aircraft in pursuance of any legal power in order to search those premises and for the duration of the search.
• Stopping a person in a public place in order to ask them to account for their actions in order to establish their possible involvement or otherwise in an offence.
• Deciding to conduct the search of a person, premises, land, vehicle, vessel or aircraft in accordance with code A Codes of Practice for PACE or any other statutory power.
• If you believe an interaction presents or is likely to present a risk to your safety or that of other persons present (i.e. someone threatening self-harm).
• If you are or may be required to exercise the use of force against persons or property.
• Giving a direction to an individual or group under any statutory power.
• Authorised and spontaneous armed operations (Authorised Firearms Officers (AFO's) will wear BWV at 'Overt Firearms Operations'. Such use will be governed by a separate regional Standard Operating Procedure (SOP) in accordance with national guidelines.
• Taser trained Officers when deployed to an incident whereby the potential for Taser deployment may be required.

- | |
|--|
| <ul style="list-style-type: none"> • Stop and search account. |
| <ul style="list-style-type: none"> • Obtaining victim statements. |

3.8.1 When Not to Use BWV

Not recording an incident may require explanation in court. However, in some instances it is not appropriate to make a video recording and in such cases users should record the rationale in their PNB.

Recording must be incident specific, and operators should not indiscriminately record entire duties or patrols. BWV must only be used to capture video or audio at incidents that would normally be subject of PNB entries or used as “professional observation” for use by supervisors.

All recordings can be used as evidence, even if at the time it appears to the user that this is unlikely, e.g. a stop and search with a negative result. All recordings should be treated as evidential until confirmed otherwise. If it becomes obvious that the recording will not be evidential, unless there are other extenuating circumstances, BWV users should stop recording immediately.

BWV users should capture as much evidence as possible including the context of the encounter and should always try to record as much of an incident as possible.

BWV users should begin recording at the start of an incident or at the earliest opportunity thereafter, for example as soon as:

- You are deployed to an incident.
- You become aware that any other encounter is likely to occur in front of you.

Examples where BWV use is <u>not</u> appropriate (for guidance only, this is not an exhaustive list)
• Intimate searches – <i>Never</i> video or make photographic recordings of intimate searches or other circumstances where persons are in a state of undress.
• Formal investigative interviews (e.g. interview for evidence-in-chief purposes, or a significant witness interview for the purpose of preparing a statement), nor for interviewing suspects as it would contravene PACE Code C.
• Rape or Serious Sexual Assault – please see section 5.8 when dealing with such reported cases.
• Legal privilege –be careful to respect legal privilege and never record material that is or is likely to be subject of such protections. Private dwellings – Always consider the right to private and family life (article 8 of the Human Rights Act) and never record beyond what is necessary for the evidential requirements of the case.
• Vulnerable Witness Interview (VWI) - the use of BWV is not a replacement for VWI and vulnerable victims, they must still be dealt with in accordance with the current force policy.

- Exercise care in using BWV where it may cause serious offence (e.g., during religious worship).
- Explosive devices – Never use in an area where it is believed that explosive devices may be present, BWV cameras could trigger explosive devices by causing electrostatic interference.

4. ROLES AND RESPONSIBILITIES

4.1 BWV Users	• Familiarise yourself with this policy and comply with it. • Ensure you have completed the necessary training prior to utilising the cameras and software. • Take responsibility for what you have chosen to record or not, which sometimes is dictated by events as they happen. Ensure you record your justification in your PNB as you may have to justify your decision during any subsequent court or other investigative proceedings. • Familiarise yourself with the 7 Key principles for the overt use of body-worn video. • Only utilise North Wales Police purchased Body Worn Videos. <u>Never</u> use any privately owned BWV device to capture evidence. • Under no circumstances should BWV be used for personal use or gain.
4.2 Local Supervisors / Custodian	• Ensure this policy is being correctly applied. • Ensure users complete the necessary training. • BWV Custodian is responsible for issuing and recovering BWV devices upon moves and changes to staffing. • BWV Custodian is responsible for reporting faults and issuing replacement BWV devices.
4.3 Systems Administrator / Information Asset Owner	• SSF HR Employment Services to set up users and provide them with logon details; completed via Systems Access Rights form. • Report any malfunctions to the relevant department (including LPS and Professional Standards Department). • Manage the DEMS database which contains the master copy of all footage.

5. THE PROCESS

5.1 Requesting and Issuing a Body Worn Video Device

Role	Action Required
5.1.1 Police Officer	• Submit a request to the custodian for a BWV device. Upon receiving your BWV • Complete any necessary training. • Familiarise yourself with this policy and the useful do's and don'ts/hints and tips available on SharePoint.

	• Ensure you DO NOT reset your BWV device using a Pin/Paperclip as this will damage the device. • Ensure you DO NOT move the docks as this will 'slow/stop' the transfer of data • Ensure you DO NOT shutdown the Dems Computer as it will stop/delay downloading. • Report any faults to CGI on 4100 and follow their instructions. • If you move to a post which doesn't require a personal issue BWV device, return your BWV device to the custodian/local supervisor.
5.1.2 Custodian / Local Supervisor	• Receive a request from an officer for a new/replacement BWV device. • Complete form C on the BWV SharePoint site and submit to the BWV department. • If an officer moves to a post where a personal issue BWV device is not required; complete form A on the BWV SharePoint site and return it along with the device to the BWV department.
5.1.3 BWV Department	• Determine whether the request is from an officer who should receive a personal issue BWV device or should be given access to a pool BWV device. Personal Issue BWV Devices • Receive the completed form C requesting a BWV device. • Allocate a personal issue BWV device in DEMS and record the Officers Collar Number. • Send the BWV device to the custodian and confirm by email that the device is on its way. Pool Issue BWV Devices • Receive the completed form C requesting a BWV device. • Allocate a pool issue BWV device in DEMS and record the Officers Collar Number. • Receive all returned BWV devices and de-allocate on DEMS and keep the BWV devices in stock for re-allocation. • Manage the return/replacement of BWV devices with Supplier.

5.2 Recording an Incident

Role	Action Required
5.2.1 BWV User	• Wear BWV when on operational duty. • Decide whether to record any incident or not (Mandatory for all DA/DV incidents). • Switch camera on when footage might support 'professional observation' or would corroborate what would be written in your PNB. • Record as much of an incident as possible as it is evidentially important to do. Therefore, begin recording at the earliest opportunity. • At the commencement of any recording or if the recording has commenced prior to arrival at the scene where practicable, make a

	verbal announcement to indicate why the recording has been activated. The announcement should include: • Date, time and location. • Incident type. • Confirmation, where practicable, to those present that the incident is now being recorded using both video and audio. • Specific words for this announcement have not been prescribed, but users should use straightforward language that can be easily understood, such as: "I am wearing and using a body worn video camera which is recording both video and sound..." • Taser Equipped Officers – All Taser equipped Officers must use BWV. In the event of a personal issue BWV not being available (due to a fault) you should contact the duty supervisor to ensure that you have access to a pool device. Priority is given to equipping Specially Trained Units (STU's) i.e. Taser officers.
5.2.2 Duty Supervisor	If no BWV is available for sign-out • Receive notification from an officer that no BWV is available for sign-out. • Give priority to equipping Specially Trained Units (STU's) i.e. Taser officers.
5.2.3 Alliance Firearms Officers	When engaged on routine operational duties • Wear BWV and adhere to this policy. When engaged on a firearms operations • Revert to the separate regional BWV SOP until you are released back to routine operational duties.

5.3 Objections to Recordings

The use of BWV is for a legitimate policing purpose and therefore in principle, you are not required to obtain the expressed consent of the person or persons being filmed.

Recording will not be ceased at the request of a member of the public.

Role	Action Required
5.3.1 BWV User	If a member of the public objects to being videoed • Inform them that the use of BWV is authorised within North Wales Police and the public should expect officers to use the equipment when dealing with incidents. If the subject of an encounter requests that the BWV be switched off • Advise the subject that :- • Any non-evidential material is retained for a maximum of 30 days only (in accordance with the Data Protection Act (DPA) and Management of Police Information (MoPI)). • The material is restricted and cannot be disclosed to third parties without the subject's express authority, unless prescribed by law. • Recorded material is police information and can be accessed on request in writing in accordance with the Freedom of Information (FOI) Act (unless an exemption applies) and is also

	accessible via a subject access request in accordance with the DPA. - Consider on a case-by-case basis whether or not to switch the BWV off. There should always be a tendency to record (within the confines of legislation) unless circumstances dictate otherwise. If you feel the recording is unnecessarily inflaming a situation - Use your judgement following the principles of the National Decision Model. If you deem it necessary to turn off your BWV, but events subsequently develop that require further investigation or proceedings: - Resume recording to capture any potential evidence. - Make the appropriate verbal announcements as noted in section 5.1.1. - Record the circumstances in your PNB.
--	--

5.4 Public Requests to Record

Users may encounter members of the public who specifically request that an encounter or interaction is recorded, even if the user does not feel that there is any evidential reason to do so.

- Record such an encounter (unless there are clear reasons not to)
- Remind the person requesting the recording that, unless there is an evidential reason to retain the footage, it will be automatically deleted in line with existing local guidelines (it will not be retained for longer than 30 days.)

5.5 Collateral Intrusion

Role	Action Required
5.5.1 BWV User	- Attempt to minimise collateral intrusion by restricting recording to areas and persons necessary (as far as is practicable) to obtain evidence and intelligence relevant to the incident. Any persons recorded as part of a Policing incident can and may be deleted from the footage by authorised and trained professionals - Note this process will be carried out in exceptional circumstances only and not as a matter of course. Decisions surrounding this process will be taken on the sensitivity of the footage captured. - The process of deleting someone from footage should be carried out by the Imaging Unit, Crime Services. - Contact them via their force email address imaging@northwales.police.uk

5.6 Private Dwellings

Role	Action Required
5.6.1 BWV User	In any private dwelling, you may find that one subject objects to the recording taking place (e.g. domestic incidents). In such circumstances

	• Continue to record and explain the reasons for recording continuously, include:- • That an incident has occurred requiring police attendance. • That your presence might be required to prevent a Breach of the Peace or injury to any person. • The requirement to secure best evidence of any offences that have occurred, whether this is in writing or on video. The video evidence will be more accurate and of higher quality and therefore in the interests of all parties. • Continuing to record will safeguard both parties with true and accurate recording of any significant statement made by either party. • An incident having previously taken place may reoccur in the immediate future. • Continuing to record will safeguard all parties against any potential allegations.
--	---

Filming in domestic circumstances can be an issue with some cultural and religious beliefs. An example may be where a female in her home may not be dressed as she would usually be in public e.g. wearing head or face coverings. Officers should be aware of this fact and be practical and sensitive to the wishes of those involved in these incidents.

5.7 Forced Entry into Premises as part of a Warrant

Role	Action Required
5.7.1 BWV User	• Capture on BWV, as a minimum :- • the initial contact with the occupants to confirm powers of entry/warrant etc. • method of entry. • Any subsequent damage to doors. This assists in any subsequent enquiries relating to the circumstances and impact of these incidents.

5.8 Crime Scenes

Role	Action Required
5.8.1 BWV User	• Capture a slow 360 degree of all crime scenes linked to serious offences. • Provide a running commentary, where possible, of factual information to assist later viewers. • Ensure the footage captures all persons present (including members of the public). This provides the Senior Investigating Officer (SIO) with previously lost evidential data and introduces savings during the investigative process. • Highlight each crime scene recorded as evidential data. • Bring it to the attention of the SIO at the earliest opportunity.

Officers must be aware that the following list is not exhaustive, and it is at the discretion of the Officer if they choose to record a full 360-degree capture of any scene.

- Murder
- Serious Assaults
- Unexplained deaths
- Suicides
- Domestic Assaults
- Criminal Damage
- Road Traffic Collisions

5.9.1 Use of BWV in Reports of Rape or Serious Sexual Assault, Child Abuse and Domestic Abuse.

- The use of Body Worn Video is mandatory for attendance at all Domestic Abuse/Violence incidents. Any decision not to use BWV should be recorded.
- Body Worn Video is a good and effective evidence gathering tool that can show in seconds what could take hours to write.
- The presumption should be in favour of recording DASH Risk Assessments with the option not to record if that is what the circumstances require, with the recording of the rationale not to record being captured. Best practice would be to do so on BWV camera where possible.
- The task for policing is to gather all the evidence in an investigation, whether or not it is supportive of the case – we should not choose to ‘not’ record because a RASSO victim might not present in the way that juries might expect, however, it is important that first responders should limit questioning to establishing only the basic facts and should leave in-depth questioning to specialist trained investigators.
- The evidence from first accounts can be the most valuable and it is these that should be recorded on BWV.
- All of the safeguards that would normally apply to the evidence from children should continue to be applied.

5.9.2 Anonymity

There are times when audio and visual footage assist in reported cases of rape; however, the importance of **anonymity** for a victim is of paramount importance.

There are instances, particularly with stranger or acquaintance rape where the offence has taken place away from the victim’s home, but the victim later reports it from their own home. In these cases the use of BWV could record details of part of the outside/inside of the victim’s home which could lead to the disclosure of private information to the defence counsel. In such cases :-

- request advice from the North Wales Police Rape Investigation Team (Amethyst), with a view to Scientific Support Unit (SSU) Imaging removing the visual part of the footage, but retaining the audio.

Conversely, if its reported as a domestic rape or where the parties are known to one another and/or the address is a crime scene the use of BWV (both audio and visual) would be beneficial to the investigation.

5.9.3 Explicit and Informed Consent

The explicit and informed consent of victims of rape and serious sexual offences should be obtained ***before*** their initial accounts are recorded on a BWV. Where the emotional or physical condition of a victim to a serious sexual offence is such that there is any doubt about their capacity to give informed consent, BWV should not be used.

5.9 Use of BWV in Mental Health Units

Section 12 of the Mental Health Units (Use of Force) Act 2018 requires all police officers attending a Mental Health Unit while on duty to assist staff that work in that unit to have their Body Worn Camera operating at all times when reasonably practicable. Please refer to [Section 12 of the Mental Health Units \(Use of Force\) Act 2018](#) for further information.

5.10 Concluding a Recording

Unless the Post Incident Procedure is invoked it is considered advisable that the officer continues to record for a short period after the incident. This will clearly demonstrate to any subsequent viewer that the incident has concluded and the user has resumed other duties or activities.

Recording may also be concluded when the officer attends another area, such as a custody unit, where other recording devices are able to take over the recording. Officers must be aware that not all areas of these departments are covered by CCTV. It is therefore at their discretion if they are to record any incidents within these areas, such as escorting prisoners to cells not containing CCTV. This may include the decision to continue recording a detained person whose behaviour requires capturing for evidential purposes.

Role	Action Required
5.10.1 BWV User	<i>Prior to concluding recording</i> - make a verbal announcement to indicate the reason for ending the recording this should state, when practicable:- - Date, time and location. - Reason for concluding recording.

5.11 Post Incident Procedure

5.11.1 What is a Post Incident procedure?

Post incident procedures commence in all situations where, following police contact, death or serious injury has occurred.

Investigations may be conducted by the force professional standards department or an Independent Investigatory Authority (IIA), such as the Independent Office for Police Conduct (IOPC). Investigations may also be undertaken by the Health and Safety Executive.

5.11.2 Initial Action

Where it is evident that following contact with police, a person has been critically/seriously injured, the Force Control Room should be contacted immediately.

Role	Action Required
5.12.2.1 BWV User	Continue recording until you are told otherwise. If the BWV was not turned on at the time injury occurred it must be as soon as practicable. The BWV recording will provide corroborating proof of the delivery of the conferring warning at/near the scene (usually by the Force Incident Manager (FIM)) as soon as practicable once the

	scene is secured, as well as evidence of the scene itself. NOTE; this is your corroborating evidence and is not a mechanism for recording the scene on behalf of the investigating bodies. Recording by Key Police Witnesses (KPW) involved in the incident en-route to the post incident location also provide confirmation that officers are not conferring about the incident in transit. This also applies to any officer not connected to the incident but escorting the KPW(s) to the Post Incident Procedure (PIP) location. On arrival at the Post Incident Suite - Continue to record until directed by the Post Incident Manager (PIM). If there are extenuating circumstances, for example you are injured / traumatised and require medical intervention. The PIM should be informed of this fact so early consideration for the need to continue to record can be assessed. <u>In cases of officer welfare and privacy</u> - You may cease recording but justification must be recorded appropriately.
5.12.2.2 PIM	- Consider the need for BWV users to continue recording once they have arrived at the PIP location, is it justified and that it doesn't does it impinge on their rights to privacy and legal privilege. - Consider carefully the requirement to balance the needs of the officers and the need for a transparent and open PIP process. - Consider the need for BWV users who have remained at the scene to continue recording, consult with the necessary investigating bodies to make a decision as to whether recording should continue or not - Once you have directed the recording to cease, record this in the PIM log. - Once recording has ceased, adhere to the process for data retrieval.

5.11.3 Post Incident Accounts

5.12.3.1 Stage One – Situation Report

Once it becomes apparent that due to police contact, a fatal / serious injury has been sustained to a third party, the force control room must be informed immediately. The information provided from the scene should be sufficient to provide a situational report which will enable the Force Incident Manager to manage the ongoing incident and assist them to discharge their responsibilities.

5.12.3.2 Stage Two – PIM Basic Facts

Role	Action Required
5.12.3.2.1 PIM	Establish the basic facts of what happened. Where possible, this information should come from a source other than a key police witness. This is most likely to take place at the nominated post incident location, where the basic facts will be provided by an individual who is willing to supply them. The basic facts will be provided (subject to legal advice where appropriate) in either verbal or written format. A staff association representative may also be

	present. The basic facts obtained by the PIM should, where possible, be sufficient to: • confirm which officers were at the scene • describe in brief the role(s) of those at the scene • confirm whose direct actions led to the injuries sustained. • Confirm the basic facts recorded or received with the person providing them to certify accuracy, • Time, date and sign the information. • Hand the original record to the independent investigatory authority at the earliest opportunity. • Retain a copy and give a copy to the person providing the basic facts. Basic facts from the key police witness Where the only person able to provide the basic facts has been, or may be, identified as a key police witness, • Offer them the opportunity to take legal advice before obtaining the information • Be aware of the need to take only basic information • Record, date and time all information provided.
--	--

5.12.3.3 Stage Three – Personal Initial Account

Role	Action Required
5.12.3.3.1 Police Officers / PCSO at the scene	• Subject to legal and medical advice, provide a personal initial account before going off duty. This should consist only of your individual recollection of events and should be written, signed and dated. The purpose of this being to record your role and what you believe to be the essential facts and should, where relevant outline the honestly held belief that resulted in your use of force. •

5.12.3.4 Stage Four – Detailed Account

Detailed accounts should not normally be obtained immediately. They can be left until the officers involved are better able to articulate their experience in a coherent format. This is usually after at least forty-eight hours. The detailed account should include, if relevant, why the witness considered the use of force to be absolutely necessary.

Officers will not be permitted to view their own or other officers BWV footage prior to the recording of their initial account (Stage 3) but will be permitted to view BWV footage prior to recording a detailed account (Stage 4); this is to protect the integrity of the process and the integrity of their evidence.

Viewing of the BWV footage after the stage 3 personal initial account will be under the direction and supervision of the appointed investigative body, for example, the IOPC or CPS and PIM.

The Post Incident Process must be open and transparent and capable of withstanding scrutiny. If any officer has concerns that the integrity of the process is not being maintained, they must immediately bring this to the attention of the PIM.

5.12 Stop & Search

Role	Action Required
5.12.1 BWV User	Video record all 'stop and search' encounters unless the search is a more thorough search or a search involving the exposure of intimate body parts as defined in code 'A' PACE 1984 code of practice. A video recording does not replace the need for compliance with the stop and search policy and code A of PACE 1984.

5.13 Selective Capture and Book Marking

Selective capture does not involve deleting images, merely making a choice of when to record or not. It also describes the process of temporarily stopping and restarting recording in order to 'bookmark' recorded footage. This breaks the digital file into chunks, making reviewing and sharing with defence and CPS easier. However, officers must be aware that stopping a recording during any Police Incident may require an explanation at court.

It is never justifiable for a user to delete images already recorded. Such action may result in legal or disciplinary proceedings. The BWV hardware used by North Wales Police is fully auditable and any deleted recordings or removal of any part of the camera is automatically reported to the systems administrator.

5.13.1 Selective Capture

Selective Capture is a phrase to cater for the choices made by officers about which elements of an incident to video. In general, users should record entire encounters from beginning to end without the recording being interrupted. However, the nature of some incidents may make it necessary for the user to consider the rationale for continuing to record throughout entire incidents.

For example, the recording may be stopped in cases of a sensitive nature or if the incident has concluded prior to the arrival of the user. In all cases the user should exercise their professional judgment in deciding whether or not to record all or part of an incident.

In cases where the user does interrupt or cease recording at an ongoing incident they should record their decision on video and in their PNB including the grounds for making such a decision.

5.13.2 Book Marking

Book marking is a means by which users may separate encounters with each of these types of person or occurrence in order to allow for easier disclosure at a later time. When recording an incident it is likely that BWV users will encounter victims, offenders and witnesses as well as recording visual evidence of the scene itself.

For example if a police officer has recorded an encounter with a witness including disclosure of their name and address this section should **not** be shown to the suspect or their legal representative.

It is recognised that Book Marking is not always practicable due to the nature of incidents and therefore this should only be attempted if the situation is calm and the operator can do so easily.

Prior to any temporary suspension for the purpose of Book Marking, the user should make a verbal announcement for the purpose of the recording to clearly state the reason for

suspending recording. The user should also announce that they have recommenced recording at the same incident as before.

The book marking process results in short breaks between clips of just a few seconds. When creating an evidential copy disk exhibit for court, the user must include all bookmarked sections for the incident, as one complete evidential copy recording of the incident.

5.14 Capturing Images of CCTV / Phone Footage on Body Worn Video Cameras

It is understood that some forces are routinely capturing images from mobile phones, CCTV screens/monitors with BWV cameras. However, then fail to go on to seize or obtain the original recording in line with CPIA requirements as the 'Master Recording'. This can present legal issues when cases arrive at court.

Taking a video or image of CCTV footage on body-worn video or other mobile device may be seen as a pragmatic way to assist with reasonable lines of enquiry whilst waiting on a formal evidential download to be completed. It does however have the potential to create significant procedural difficulties and should only be considered for immediate intelligence purposes only (for example, where there is an immediate threat to life or to facilitate recognition of an offender at large). It **must** always be followed up with a valid download of the original image data.

Key points

- The use of BWV to capture video or images from any another device is only seen as a last resort in response to immediate intelligence purposes for recognition only.
- Officers must ensure that if this is done, the original source recording must also be seized and treated as an exhibit in line with current working practices.

5.15 Witness First Accounts

Role	Action Required
5.15.1 BWV Users	If approached by victims or witnesses who are giving their first account of the crime :- • You may record the encounter using BWV but consider the needs of the individual with regards to sensitivity based on the nature of the offence being reported. Any initial disclosure from victims and witnesses recorded by BWV • Treat as an evidential recording. • Submit to the investigating officer, this is important to ensure compliance with statutory identification procedures under PACE Code D. • Recordings do not replace the need for formal written statements from victims or witnesses but they can be used as supporting evidence for the statements and can also be considered as hearsay evidence and used in accordance with the provisions of the Criminal Justice Act 2003.

	• If a recording relates to the victim's first notes or initial description of suspects :- • Refer to the relevant section of the video when making their written statement. • Take care to ensure that the witness reviews only their account. They must not be allowed access to other sections of the recording. • Record in the witness statement the extent of any review by the witness to assist with making their statement.
--	--

5.16 Recording of Interviews

Never use BWV to record interviews of suspects under caution which occur at a police station.

5.17 Witness Identification

Witnesses to a Policing incident where the offender is present should under no circumstances be shown the video captured on the BWV. Officers should revert to [Police and Criminal Evidence Act 1983 Code D](#)).

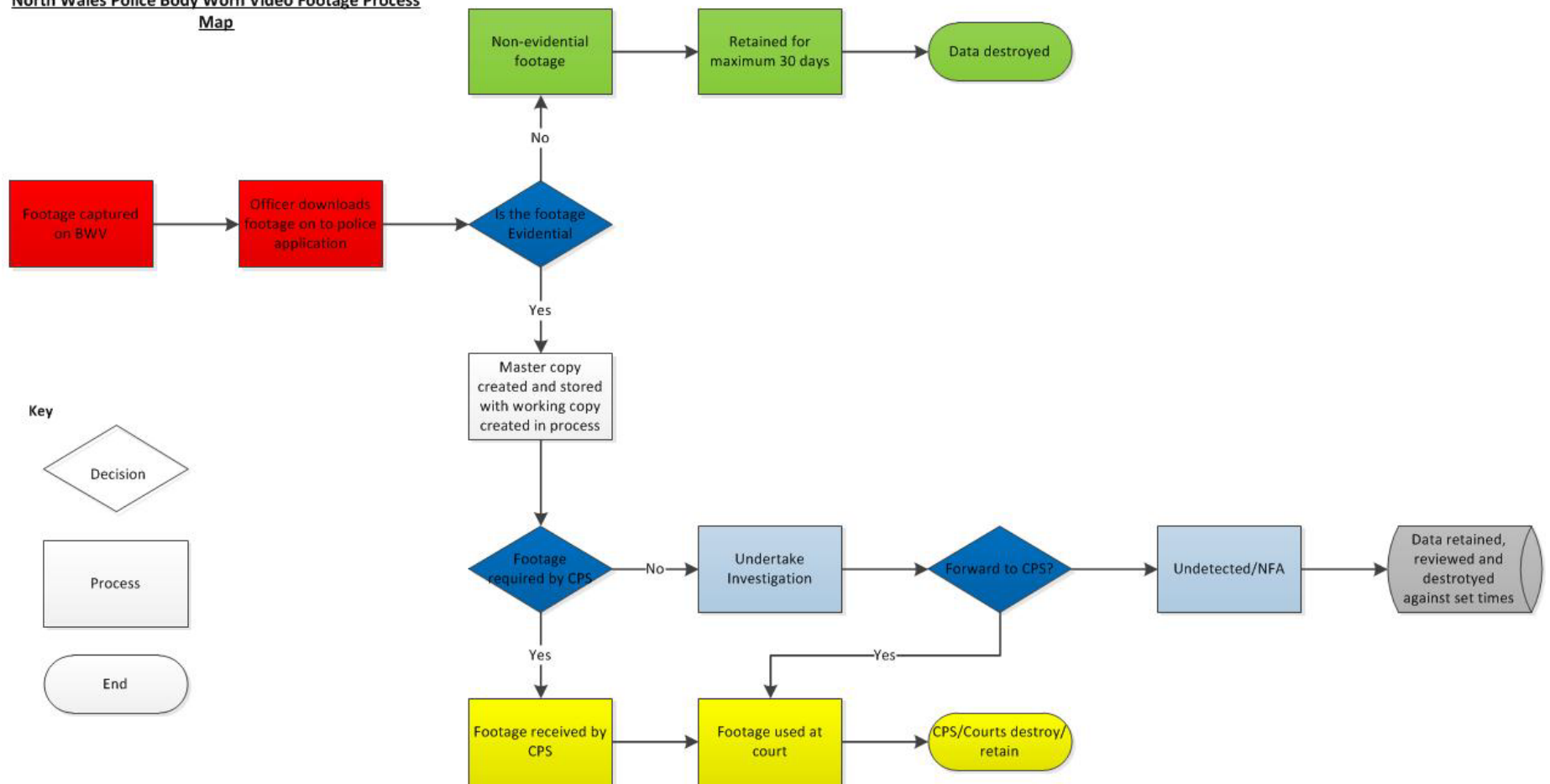
5.18 Uploading, File References and Exhibits

All footage recorded to the BWV device must be downloaded at the end of the officer's tour of duty and the device returned to the docking computers at the officers' home station.

Once downloaded, the camera is clear of all footage and ready to be booked out again.

All recorded footage is automatically downloaded and saved on the secure networked data storage facility.

North Wales Police Body Worn Video Footage Process Map



5.18.1 Evidential Footage

Evidential footage is considered any data that :-

- provides evidences of an offence.
- Supports evidence for any process - i.e. charge, Fixed Penalty Notice, Penalty Notice for Disorder etc.
- Is required for a relevant and proportionate policing purpose - i.e. footage taken of an overcrowded town centre taxi-rank to highlight the need for an extended facility to Local Authority partners.
- Should be revealed under The Criminal Procedure and Investigations Act 1997.

Never download data to any device other than through the dedicated BWV docking computers provided. Any attempt to do so will result in the automated reporting of such an attempt. Any user found doing so, may be liable for prosecution or disciplinary procedures.

5.18.2 Burning evidential footage to DVD (working copy) for submission to AJD (and then CPS)

The CPS request that whenever possible footage clips are not cropped as the defence may ask for the full version.

Role	Action Required
5.19.2.1 BWV Recording Officer	• Ensure that evidential footage is correctly downloaded and that the Unique Reference Number (URN) for the footage is fully recorded on the associated NICHE Record. • Identify any saved evidential footage by entering the NICHE Crime or iCAD log number in the incident ID column and other details such as exhibit number, suspects and other relevant details in the notes column. • Ensure you add the URN and other details to the disc as soon as it is burned off. Failure to do so may result in the disc not being linked to the case file. • Complete the MG5 with details of the officer/s making the recording, timings and summary; the summary should be such that what the evidence captured on the disc is accurately and fully described. If BWV is supporting evidence • You are still required to provide written statements, including the audit trail for the capture of the footage and the subsequent production of the master disc/DVD.
5.19.2.2 Officer in Charge (OIC)	• Ensure that any appropriate footage is made available in a format that is suitable to the requirements of where it is to be played (e.g., currently, Courts require DVD versions of footage, so you need to ensure that the footage is burned onto an appropriate disc). If more than one BWV device is present at the scene of an incident or if the area of the incident is also covered by a CCTV system • Ensure that all available footage of the incident is secured as exhibits in consideration of any defence arguments that may be presented.

Data downloaded as non-evidential will be stored on the Digital Evidence Management System (DEMS) for 30 days. During that time it is searchable and can be retrieved and marked as evidential. After this period it will be automatically deleted.

5.19 Requests for Editing or Producing CD/DVD's - Imaging Unit - Crime Services

The Imaging Unit (Crime Services) is responsible for managing the DEMS database which contains the master copy of all footage. Furthermore the department is the administrative centre for BWV in respect of the systems management of DEMS. All requests for footage editing or DVD production assistance should be made through SSU Imaging Unit.

5.20 Officers Viewing Footage Prior to Making a Statement

Role	Action Required
5.20.1 Officers making a statement	You may view any BWV footage prior to completing a written evidential statement. However it is recognised in very rare circumstances BWV may be required and therefore seized as part of an enquiry into the most serious of incidents (e.g. an incident involving the death or serious injury to a member of the public).

5.21 Use by Professional Standards Department (PSD)

North Wales Police PSD do not dip sample or routinely view BWV footage material.

BWV footage is subject to the principles outlined in the Data Protection Act, this prohibits the random dip sampling of retained footage other than for supervision and / or investigation purposes. Open access to any database or server containing BWV footage for reasons other than this will not normally be granted unless exceptional circumstances exist and authority is given by the Head of Professional Standards.

Footage from incidents can be used to identify poor performance and learning opportunities. BWV footage can be used to quickly resolve complaints and avoid lengthy investigations. There is strong evidence to support the fact that BWV contributes to a net reduction in complaints and subsequent disciplinary action, by providing a clear and impartial record of any interaction.

This means that when a complaint arises the video record can be used to quickly establish exactly what happened and provide a speedy resolution as part of the complaints process. This provides greater transparency, and allows officers to show that they followed the correct procedure if their actions are challenged.

Material not directly relating to investigation should not be made available to the investigating officer.

PSD must create master and working copies of any BWV material used in an investigation of a complaint and retain these in secure storage in accordance with force procedures.

All complaints received from the public about the conduct of any officer or member of staff (including those subsequently withdrawn) must be recorded in accordance with existing national and force procedures.

Where a complaint is dealt with by local resolution, the local supervisor should make a record of the viewing.

Role	Action Required
5.21.1 Investigators	- Only access footage for professional standards purposes where there is a clear and justifiable need to do so (e.g., specific investigations, identified patterns of complaints in respect of a particular officer) or where specific intelligence has been received that would indicate that viewing of BWV footage is proportionate and necessary. - When reviewing footage make a note of the fact you have done so and a brief reason for reviewing the particular piece of footage. - Record any viewing of footage by complainants. - Consider whether non-connected persons on the material should be obscured when being viewed by complainants/third parties. - Secure, review and retain BWV material that is relevant to the investigation of any complaint at the earliest opportunity, in line with the parameters of the investigation
5.22.2 Supervisors	- Consider reviewing BWV footage relating to your officers as a supervision tool and as a means of improving performance or to identify training needs. This is especially important in areas such as stop & search, where improved performance will increase community confidence. - When reviewing footage make a note of the fact you have done so and a brief reason for reviewing the particular piece of footage.

5.22 Provision of Data to Outside Organisations

Never provide or send system data outside of the Force **without** prior permission from the System Owner/Information Asset Owner and/or the NWP Chief Information Officer.

Data sent outside the Force must be compliant with :-

- the Data Protection Act,
- The Management of Police Information (MOPI) guidance,
- Government Security Classification Scheme (GSCS)
- The Force [Information Sharing procedure](#) (within the [Force information Standards Policy](#)).

Relevant documentation must be completed therefore prior to sharing, you must seek advice from the Information Standards and Compliance Department to ensure the requirements within relevant legislation are met. In all cases you must mark the information appropriately in accordance with the [Government Security Classification Scheme](#), including a suitable handling rule where necessary.

5.23 Body Worn Video in Public Order Deployments

BWV currently deployed within Local Policing Services, can be used during public order deployments, but must only be used in a response function, namely incident specific when dealing with personal interactions.

- BWV must not be deployed as a pseudo Evidence Gathering Team (EGT) tactic.
- BWV should only be used to capture an officer's personal interaction with another as per the national BWV guidance.
- BWV is used in public order deployments, specific briefings with regards to its use must be given.
- After activating the BWV officers must give their name, rank and force number along with a rationale for switching the BWV on if practicable to do so, for

example when delivering a 'five step appeal'. BWV should only be switched off once that interaction has concluded and where practicable the officer should verbalise that the BWV is being switched off.

Role	Action Required
5.23.1 Public Support Unit (PSU) Commanders	Consider the public perceptions and community impact of BWV in public order deployments: the effect on others within the event, both in relation to collateral and crowd dynamics; the effect on perception before and during peaceful protest; and ultimately its impact on public confidence.

5.24 Mutual Aid

- **Before** being deployed on mutual aid, the requesting force must advise whether or not they have compatible downloading provisions for the responding force BWV system.
- Where data from the BWV camera is downloaded within the requesting force area, the Chief Constable of that area will fulfil the duties of data controller ensuring compliance with legal obligations under the Data Protection Act.
- Alternatively, should footage need to be downloaded within the responding force area, the Chief Constable of this force will fulfil the duties of data controller.

5.25 Retention & Disposal

Information in relation to the retention and disposal of information can be found in the [Information Management section of APP](#).

5.25.1 Retention and Legislation

All CCTV and digital media evidence must be retained / disposed of in accordance with the Human Rights and Data Protection Act.

5.25.2 Disposal

All media at the conclusion of its appropriate evidential lifecycle must be considered for recycling /destruction. CD/DVD's must be shredded and disposed of in accordance with existing force policy.

6. DECLARATION & LEGALITIES

- 6.1** In line with all Force policies, the overarching purpose of this document is to directly support the PCC police and crime plan objectives. Overall the intention of this policy is to provide a safer North Wales.
- 6.2** In the writing of this policy cognisance has been taken of the college of policing code of ethics (2014).
- 6.3** North Wales Police policies will be written in accordance with the approved corporate format and published on the Force Intranet, allowing access to staff and public, where appropriate, on the pages of the public facing Internet site under the Force publication scheme and Freedom of Information Act 2000.
- 6.4** The following main legal requirements have been identified within this policy:
 - Equality Act 2010
 - Human Rights Act 1998
 - The Welsh Language (Wales) Measure 2011 and the Welsh Language Standards for the Chief Constable

- Data Protection Act 2018
- Freedom of Information Act 2000
- Health and Safety Act 1974
- European Convention on Human Rights
- Protection of Freedoms Act 2012
- Police and Criminal Evidence Act 1984
- Serious Organised Crime & Police Act 2005

6.5 This policy has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA).

6.6 New legislative requirements or changes in Force structure may necessitate a review of this policy document.

FOR IS&C USE ONLY

Summary of actions and finding

		Tab Number				
Area		1	2	3	4	5
Processing	Legislation					
	Consent requirements					
	Logging					
	Automated Decision-Making					
Retention	Retention					
Special category/Sensitive Processing	Legislation					
Security	Security					
Location of data	Location of data					
Data Processors	Contracts					
	DPA					
Information Sharing	ISA's (incl audit trails)					
Privacy Notices	Privacy Notice Content					

DPIA	DPIA					
Personal Data Breaches	Personal Data Breaches					
Other relevant areas	Requesting information					
	Policy					
	Training					
	IT System Compliance					
	Misc items					

Key			
	Mandatory field		
	Optional field		
	Additional NWP field		
Team Name:-	Surveillance		
Return completed by:-	...	Date	27.8.2019
Process (Work Stream) Overview			
Department	Name of Process & Brief Description of Process	Personal Data	Purpose of processing
CS - Surveillance Unit	Surveillance The process of gathering evidence and intelligence using surveillance (all authorised methods) to support criminal investigations	Yes	More than one of the Policing Purposes

		Data Collection	
Name and contact details of joint controllers (if applicable)	GDPR/LEP	Source	Transfer method IN
N/A	LEP	Most/all of the above	Internal

Fair Processing Notice/ Privacy Notice	Categories of individuals	Categories of personal data	Legal Basis
Subject not aware	LE - Suspects, offenders, victims, associates	LE -All/most of the above	Article 6(1)(e) - public interest task

Processing			
Relevant Legislation	Location of record of consent	Consent Requirements Met?	LEP ONLY Logging requirements met? S62 DPA 2018
Part III Police Act 1997 RIPA Part II 2000 R v Sutherland 2002	N/A	N/A	Yes - all

	Retention	
Automated Decision Making and Profiling	Retention schedule (if possible)	Lawful basis for processing Special Category Data Please provide the actual legislation in column M (Relevant Legislation)
N/A	12 months in office then Force Records	Law enforcement purposes

Data Protection Act 2018 - Special Category or Criminal Con

GDPR Article 9 lawful basis for processing	SUBSTANTIAL PUBLIC INTEREST Additional conditions when relying on Substantial Public Interest (DPA 2018 Schedule 1)	CRIMINAL DATA Additional conditions required for Criminal Data (DPA 2018 Schedule 8)
Not applicable	Not applicable	Sch.8, 1 - Statutory purposes

viction and Offence data		
Link to retention and erasure policy document	Is personal data retained and erased in accordance with the policy document?	Reasons for not adhering to policy document (if applicable)
Data Protection - Sensitive Data Processing Policy	Force Records manage this	N/A

Security	Access Requests	
General description of technical and organisational security measures (if possible)	Location of personal data/Systems	Categories of recipients (see Section 8 of NWP Privacy Notice for examples)
Ongoing confidentiality, integrity, availability and resilience	Locked cabinet in Office then force Records/Archive after 12 months All other information passed to Investigation team	Partners in the Criminal Justice arena

Transfer		
Internal Transfer	External Transfer	Information Sharing Agreement
To investigating team either by hand, internal email or via RMS. Some intel may be shared via normal Intel route - submit CID 56	To CPS via secure email when requested	ISA - Not Required

Details of Data Processor	Names of third countries or international organisations that personal data are transferred to (if applicable)	Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable)
N/A	N/A	N/A

Location of Privacy Notice	Article 6 lawful basis for processing personal data	Additional condition for processing special category/sensitive data
Force Privacy Notice	Force Privacy Notice	Force Privacy Notice

Privacy Notice Content	
Legitimate interests for the processing (if applicable)	Link to record of legitimate interests assessment (if applicable)
Force Privacy Notice	N/A

Rights available to individuals	Existence of automated decision-making, including profiling (if applicable)
Force Privacy Notice	Force Privacy Notice

	Data Protection Impact Assessment	
The source of the personal data (if applicable)	Data Protection Impact Assessment required?	Data Protection Impact Assessment progress
Force Privacy Notice	NO	N/A

ments	Personal Data Breaches	
Link to Data Protection Impact Assessment	Has a personal data breach occurred?	Link to record of personal data breach
N/A	No	N/A

Describe what local department procedures/guidance you have in place.	Comments
Information Security Incident Procedure	

Example

Key	
-----	--

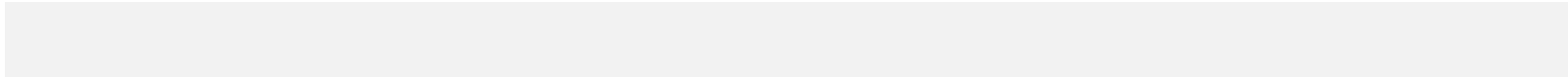
	Mandatory field
	Optional field
	Additional NWP field

	Process (Work S

[illegible]

Stream) Overview		
Purpose of processing	Name and contact details of joint controllers (if applicable)	GDPR/LEP
Payroll	N/A	
Payroll	N/A	
Payroll	N/A	
Payroll	N/A	
Personnel file	N/A	
Personnel file	N/A	
Personnel file	N/A	
Personnel file	N/A	
Personnel file	N/A	
Recruitment	N/A	
Recruitment	N/A	

[illegible]

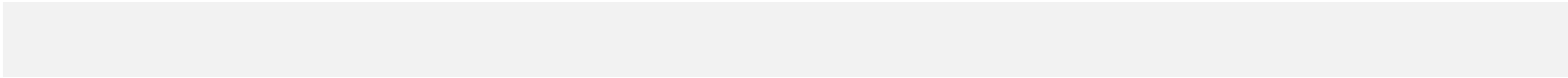


Categories of individuals	Categories of personal data	Legal Basis
Employees	Contact details	
Employees	Bank details	
Employees	Pension details	
Employees	Tax details	
Employees	Contact details	
Employees	Pay details	
Employees	Annual leave details	
Employees	Sick leave details	
Employees	Performance details	
Successful candidates	Contact details	
Successful candidates	Qualifications	

Processing

[illegible]

[illegible]



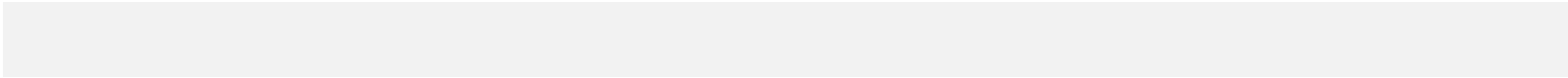
Data Protection Act 2018		
GDPR Article 6 lawful basis for processing	GDPR Article 9 lawful basis for processing	SUBSTANTIAL PUBLIC INTEREST Additional conditions when relying on Substantial Public Interest (DPA 2018 Schedule 1)
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A
Article 6(1)(b) - contract	Article 9(2)(b) - employment	Sch.1, Pt.1, 1 - Employment
N/A	N/A	N/A
N/A	N/A	N/A
N/A	N/A	N/A

Record of Processing Activities

3 - Special Category or Criminal Conviction and Offence data

CRIMINAL DATA Additional conditions required for Criminal Data (DPA 2018 Schedule 8)	Link to retention and erasure policy document	Is personal data retained and erased in accordance with the policy document?
	N/A	N/A
	N/A	N/A
	N/A	N/A
	N/A	N/A
	N/A	N/A
	N/A	N/A
	N/A	N/A
	Link	Yes
	N/A	N/A
	N/A	N/A
	N/A	N/A

	Security	Access Requests
Reasons for not adhering to policy document (if applicable)	General description of technical and organisational security measures (if possible)	Location of personal data/Systems
N/A	Encrypted storage and transfer	Finance payroll system
N/A	Encrypted storage and transfer	Finance payroll system
N/A	Encrypted storage and transfer	Finance pension system
N/A	Encrypted storage and transfer	Finance payroll system
N/A	Encrypted storage	HR personnel system
N/A	Encrypted storage, access controls	HR personnel system
N/A	Encrypted storage, access controls	HR personnel system
N/A	Encrypted storage, access controls	HR personnel system
N/A	Encrypted storage, access controls	HR personnel system
N/A	Encrypted storage and transfer	HR Recruitment system
N/A	Encrypted storage, access controls	HR Recruitment system



Tran		
------	--	--

Categories of recipients (see Section 8 of NWP Privacy Notice for examples)	Internal Transfer	External Transfer
HMRC		
HMRC		
HMRC		
HMRC		
N/A		
N/A		
N/A		
N/A		
N/A		
Referee		
N/A		

Transfer	

[illegible]

Article 6 lawful basis for processing personal data	Article 9 condition for processing special category data	Legitimate interests for the processing (if applicable)
Article 6(1)(c) - legal obligation	N/A	N/A
Article 6(1)(c) - legal obligation	N/A	N/A
Article 6(1)(c) - legal obligation	N/A	N/A
Article 6(1)(c) - legal obligation	N/A	N/A
Article 6(1)(b) - contract	N/A	N/A
Article 6(1)(b) - contract	N/A	N/A
Article 6(1)(b) - contract	N/A	N/A
Article 6(1)(b) - contract	Article 9(2)(b) - employment	N/A
Article 6(1)(b) - contract	N/A	N/A
Article 6(1)(b) - contract	N/A	N/A
Article 6(1)(b) - contract	N/A	N/A

Privacy Notice Content		
Link to record of legitimate interests assessment (if applicable)	Rights available to individuals	Existence of automated decision-making, including profiling (if applicable)
N/A	Access and rectification	No
N/A	Access and rectification	No
N/A	Access and rectification	No
N/A	Access and rectification	No
N/A	Access and rectification	No
N/A	Access and rectification	No
N/A	Access and rectification	No
N/A	Access and rectification	No
N/A	Access and rectification	No
N/A	Access, data portability, rectification	Yes
N/A	Access, data portability, rectification	Yes

	Data Protection Impact Assessment	
The source of the personal data (if applicable)	Data Protection Impact Assessment required?	Data Protection Impact Assessment progress
Data subject	No	N/A
Data subject	No	N/A
Controller	No	N/A
Controller	No	N/A
Data subject	No	N/A
Controller	No	N/A
Controller	No	N/A
Controller	No	N/A
Controller	No	N/A
Data subject	Yes	Completed
Data subject	Yes	Completed

s	Personal Data Breaches	
Link to Data Protection Impact Assessment	Has a personal data breach occurred?	Link to record of personal data breach
N/A	No	N/A
N/A	No	N/A
N/A	No	N/A
N/A	No	N/A
N/A	No	N/A
N/A	No	N/A
N/A	No	N/A
N/A	No	N/A
N/A	No	N/A
Link	No	N/A
Link	No	N/A

Key

	Mandatory field
	Optional field
	Additional NWP field

Process (Work Stream) Overview

Department	Name of Process	Personal Data	Purpose of processing
		Yes	Protecting life and property
		No (Do not proceed with assessment for this process)	Preserving Order
		Unsure (Contact IS&C to clarify)	Prevention and Detection of Crime
			Bringing offenders to justice
			A duty or responsibility of the police arriving from law

			More than one of the Policing Purposes
			Ensuring operational effectiveness
			Information sharing/partner working
			Legislative compliance
			Crime recording/stats
			Ensuring integrity
			Personnel file
			Payroll
			Recruitment
			Absence management
			Direct Marketing
			Other (see comments)

		Data Collection	
Name and contact details of joint controllers (if applicable)	GDPR/LEP	Source	Transfer method IN
	GDPR	NWP System	N/A
	LEP	NWP System/Manual Records	External - all involved in investigation (victim/witness/suspect)
	Both LEP and GDPR for Policing Purpose/sharing purposes	Officers/staff and NWP System/Manual Records	External - E-mail
	Unsure	Officers/staff	Internal and External - application forms (paper and web based)
		Public	External - Web Form

[illegible]

Fair Processing Notice/ Privacy Notice	Categories of individuals	Categories of personal data	Legal Basis
Subject aware	LE - Nominals	GDPR	Article 6(1)(a) - consent
Subject not aware	LE - Victims	GDPR - Names, email addresses	Article 6(1)(b) - contract
Subject sometimes aware/not aware	LE - Offenders	GDPR - Names, contact details	Article 6(1)(c) - legal obligation
Unsure	LE - Suspects	GDPR - Names, DOB, Address and/or contact details	Article 6(1)(d) - vital interests
	LE - Suspects and Offenders	GDPR - Identification documents / ID numbers	Article 6(1)(e) - public interest task

	LE - Witnesses	GDPR - Financial; banking	Article 6(1)(f) - legitimate interests
	LE - Victims and/or Offenders LE - Applicants	GDPR -Vehicle ie VRN	
		GDPR -Pay details	
		GDPR -Tax details	
	LE - Most/all of the above	GDPR -Pension details	
	GDPR - Suspects and Offenders	GDPR -Racial/Ethnic origin	
	GDPR - Successful Candidates	GDPR -Political, religious or philosophical beliefs	
	GDPR - Unsuccessful Candidates	GDPR -Trade Union Membership	
	GDPR - Employees	GDPR -Genetic data	
	GDPR - Contractors	GDPR -Biometric data	
	GDPR - Most/All of the above	GDPR -Photographs	
		GDPR -Disability, Mental & Physical health data	
		GDPR -Sex life and/or Sexual Orientation	
		GDPR -Annual Leave details	
		GDPR -Sick leave details	
		GDPR -GDPR Employment history	

		GDPR -Qualifications	
		GDPR -Performance details	
		GDPR -Alleged or actual offending data (Convictions)	
		GDPR - All/most of the above	
		GDPR - Name, address, dob, contact details, disability, mental and/or physical health data	

Processing			
Relevant Legislation	Location of record of consent	Consent Requirements Met?	LEP ONLY Logging requirements met? S62 DPA 2018
		YES	Yes - all
		NO - provide details in Comments at end of row	Collection
		UNSURE - refer to IS&C	Alteration
		N/A	Consultation
			Disclosure

[illegible]

	Retention	
Automated Decision Making and Profiling	Retention schedule (if possible)	Lawful basis for processing Special Category Data
N/A		Not applicable
Performance at work		
Economic situation		Law enforcement purposes
Health		
Personal preferences		(non law enforcement)

[illegible]

Data Protection Act 2018 - Special Category or Criminal Con

GDPR Article 9 lawful basis for processing	SUBSTANTIAL PUBLIC INTEREST Additional conditions when relying on Substantial Public Interest (DPA 2018 Schedule 1 - along with appropriate policy document)	CRIMINAL DATA Additional conditions required for Criminal Data (DPA 2018 Schedule 8)
Not applicable	Not applicable	Not applicable
	Sch.1, Pt.1, 1 - Employment	Sch.8, 1 - Statutory purposes
Article 9(2)(a) - Explicit consent	Sch.1, Pt.1, 2 - Health or social care	Sch.8, 2 - Administration of justice
Article 9(2)(b) - Employment, Soc. Sec, Social Protection	Sch.1, Pt.1, 4 - Research	Sch.8, 3 - Vital interests
Article 9(2)(c) - Vital interests	Sch.1, Pt.2, 6 - Statutory, common law, government	Sch.8, 4 - Safeguarding of children and of individuals at risk

Article 9(2)(d) Not for profit PPRTU	Sch.1, Pt.2,7 - Administration of justice or parliamentary functions	Sch.8, 5 - Manifestly made public by the data subject
Article 9(2)(e) - Made public by the data subject	Sch.1, Pt.2, 8 - Equality or opportunity of treatment	Sch.8, 6 - Legal claims
Article 9(2)(f) - Legal claims, judicial capacity	Sch.1, Pt.2, 9 - Racial/Ethnic diversity at senior levels	Sch.8, 7 - Judicial acts (processing by the judiciary)
Article 9(2)(g) - Substantial public interest, on basis of law	Sch.1, Pt.2, 10 - Preventing/detecting unlawful acts	Sch.8, 8 - Anti-fraud organisations preventing fraud
Article 9(2)(h) - Medical, Social Care	Sch.1, Pt.2, 11 - Protecting public against dishonesty etc.	Sch.8, 9 - Archiving
Article 9(2)(i) - Public health	Sch.1, Pt.2, 12 - Regulatory activity re: unlawful acts, dishonesty	
Article 9(2)(j) Archiving, Research and Statistics	Sch.1, Pt.2, 13 - Journalism (PI, intent to publish)	
	Sch.1, Pt.2, 14 - Preventing fraud (anti-fraud orgs)	
	Sch.1, Pt.2, 15 - Terrorist finance/money laundering	
	Sch.1, Pt.2, 16 - Disability/MH support organisations	
	Sch.1, Pt.2, 17 - Counselling	
	Sch.1, Pt.2, 18 - Safeguarding children and adults at risk	
	Sch.1, Pt.2, 19 - Safeguarding economic wellbeing of vulnerable adults	
	Sch.1, Pt.2, 20 - Insurance	
	Sch.1, Pt.2, 21 - Occupational pensions	
	Sch.1, Pt.2, 22 - political parties (political opinion)	

	Sch.1, Pt.2, 23 - Elected representatives (requests to)	
	Sch.1, Pt.2, 24 - Disclosures to elected representatives	
	Sch.1, Pt.2, 25 - Elected representatives (prisoner data)	
	Sch.1, Pt.2, 26 - Publication of legal judgements	



viction and Offence data

Link to retention and erasure policy document	Is personal data retained and erased in accordance with the policy document?	Reasons for not adhering to policy document (if applicable)

Pick lists		
Security	Access Requests	
General description of technical and organisational security measures (if possible)	Location of personal data/Systems	Categories of recipients (see Section 8 of NWP Privacy Notice for examples)
Pseudonymisation		
Encryption		
Ongoing confidentiality, integrity, availability and resilience		
Data can be restored/accessed in event of an 'incident'		
Regular testing of security		

[illegible]

Transfer		
Internal Transfer	External Transfer	Information Sharing Agreement
		ISA - Not Required
		ISA - Required but not yet written
		ISA - currently in draft
		ISA in place but needs updating
		ISA in place and current

[illegible]

Details of Processor	Names of third countries or international organisations that personal data are transferred to (if applicable)	Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable)
		Not applicable (no transfer)
		None in place
		Other department responsible for overseas transfer
		Legally binding instrument (between public authorities) in place
		Binding corporate rules in place

[illegible]

Location of Privacy Notice	Article 6 lawful basis for processing personal data	Additional condition for processing special category/sensitive data
	Article 6(1)(a) - consent	N/A
	Article 6(1)(b) - contract	Law Enforcement Purpose
	Article 6(1)(c) - legal obligation	
	Article 6(1)(d) - vital interests	Article 9(2)(a) - Explicit consent
	Article 6(1)(e) - public interest task	Article 9(2)(b) - Employment, Soc. Sec, Social Protection

[illegible]

Privacy Notice Content		
Legitimate interests for the processing (if applicable)	Link to record of legitimate interests assessment (if applicable)	Rights available to individuals
		Access and rectification
		Access, data portability, rectification
		Access, data portability, rectification, objection, erasure* *only in certain circumstances
		Access, data portability, rectification, objection, erasure*, restrict processing *only in certain circumstances
		Access, data portability, rectification, objection, erasure*, restrict processing, automated decision making including profiling *only in certain circumstances

[illegible]

Existence of automated decision-making, including profiling (if applicable)	The source of the personal data (if applicable)	Data Protection Impact Assessment required?
		YES
		NO
		UNSURE - refer to IS&C

Data Protection Impact Assessments		
Data Protection Impact Assessment progress	Link to Data Protection Impact Assessment	Has a personal data breach occurred?
N/A	N/A	YES
Completed		NO
In Progress		UNSURE
Not started		

Personal Data Breaches		
Link to record of personal data breach	Describe what local department procedures/guidance you have in place.	Comments

Notes
Use this template to document the processing activities you undertake as a controller. Headings highlighted green are required areas of documentation under Article 30 of the GDPR or Schedule 1 of the Data Protection Act 2018. Headings highlighted blue are optional areas of documentation that are not required under Article 30 of the GDPR or Schedule 1 of the Data Protection Act 2018. Headings highlighted cream are additional optional areas of documentation that are not required under Article 30 of the GDPR or Schedule 1 of the Data Protection Act 2018 (NWP)
Instructions
1. Complete your organisation's name and contact details on the first tab in cells B3 - B6 2. Complete your data protection officer's name and contact details (if applicable) on the first tab in cells D3-D6. 3. Complete your representative's name and contact details (if applicable) on the first tab in cells F3-F6. 4. Document your organisation's processing activities, starting in cell A8, and working from left to right. Where necessary use multiple rows for each processing activity in order to be as granular as possible (see example tab).
Guidance
For more detailed guidance on documentation, please see the Guide to GDPR on our website.