HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Response Date:06/05/2025

2025/494 - Information Management Strategy

In response to your recent request for information regarding;

The NWP Information Management Strategy document

Please find attached the Information Management Strategy.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 02/05/2025

HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

Force Information Management Strategy Framework

FRAMEWORK

Document Type:	**Framework**
Framework Owner:	**Chief Information Officer**
Department:	**Finance and Resources**
Framework Writer:	**Chief Information Officer**
Version:	**3.0**
Effective Date:	**30/10/2023**
Recommended Review Date:	**30/10/2025**

Version No	Date	Author	Changes
2.0		...	Change to new template format
3.0	30/10/23	...	Scheduled review and minor amendments made.

CONTENTS

1. IINFORMATION MANAGEMENT STRATEGY - BACKGROUND 2

2. INFORMATION MANAGEMENT STRATEGIC VISION 2

3. BUSINESS BENEFITS AND OUTCOMES 2

4. INFORMATION MANAGEMENT VALUES 3

4.1 The Standards: 4

4.2 Business Management: 4

4.3 People Management: 4

4.4 Information Sharing: 4

4.5 Data/Information Management: 4

5. SCOPE OF STRATEGY 5

6. EXPLOITATION OF INFORMATION 5

7. STRATEGIC OBJECTIVES 5

8. ROLES AND RESPONSIBILITIES FOR STRATEGIC INFORMATION MANAGEMENT 7

9. OPERATIONAL CONSIDERATIONS 8

10. FORCE POLICY DECISIONS FOR INFORMATION MANAGEMENT 9

11. LEGAL REQUIREMENTS 11

1. INFORMATION MANAGEMENT STRATEGY - BACKGROUND

This document defines how the strategic objectives of North Wales Police will be supported by the effective management of information. This includes the strategic vision; business drivers and benefits; guiding principles; and overall governance. This document also demonstrates the relationship between Information Management-related business areas, their strategic fit with North Wales Police's Policing Plan and the current information management programmes, projects and work-streams.

The Information Management Strategy (IMS) will set out the strategic aim of the organisation and the principles of information management. The IMS will detail the underlying standards, roles and responsibilities of key personnel in the management of information. It is the responsibility of everyone within North Wales Police to ensure information is used appropriately, in-line with this strategy and accompanying policies and procedures, in particular the Force Information Standards Policy (FISP).

2. INFORMATION MANAGEMENT STRATEGIC VISION

North Wales Police's vision is Making North Wales the SAFEST place to live, work and visit in the UK. This is the overall outcome that we, as one team, are striving to achieve.

The IMS underpins the forces aim by enabling individual's access to the information they need, when they need it, and in the appropriate form. Access to information will be straightforward, effective, secure and available in an efficient and cost-effective manner.

All our staff and partners will understand the value and importance of high quality, up-to-date and reliable information and will be properly equipped to obtain, use, maintain, and dispose of information correctly, lawfully and efficiently in support of the delivery of North Wales Police's strategic aims (Figure 1.0).

3. BUSINESS BENEFITS AND OUTCOMES

This strategy informs how North Wales Police will manage all of its police information within the policing context. It is designed to support and assist the implementation of all other Force policies and strategies. It provides the over-arching framework to implement those policies and protocols which manage information and is not a stand-alone document.

It provides a mandate for the performance of all information management functions to ensure that all staff and others, including agencies, contractors and partners involved with police information, carry out their duties competently and efficiently.

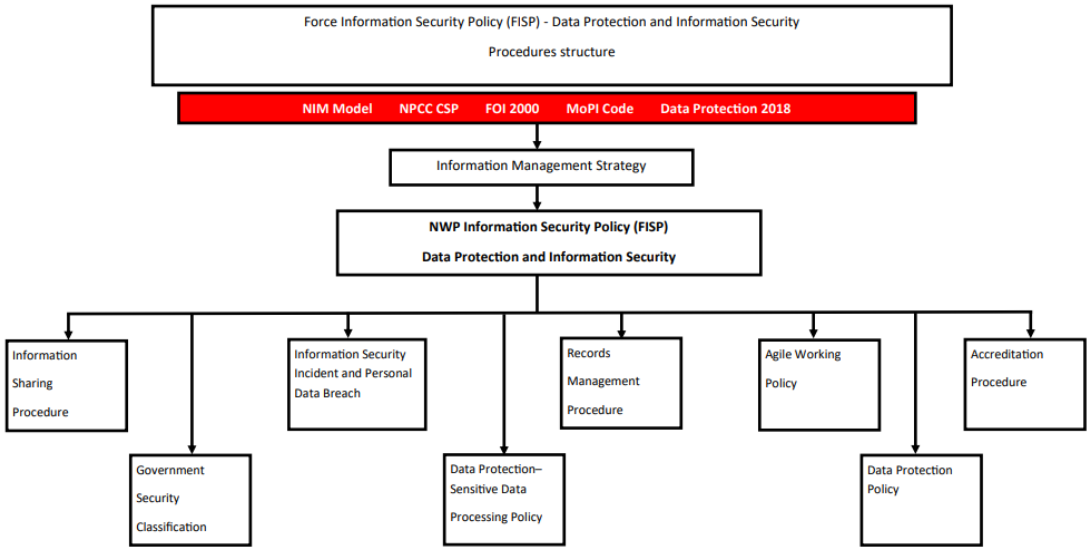
The timely provision of comprehensive, accurate, up-to-date and reliable information and intelligence is critical to enabling all staff within the Force, the wider police family and our partner agencies to fulfil their roles.

In addition, to improve public confidence and customer service the public and other stake-holders must have access to the information they need to know, both to reassure them within their communities and to ensure they are provided with a satisfactory level of service. This service delivery is underpinned by efficient and effective resource and performance management.

When combined with statutory requirements, such as the guidance within Authorised Professional Practice (APP), formerly the Management of Police Information (MoPI), there is a clear imperative to develop sound Information Management to account for each of these business requirements that directly supports the Forces' Strategic Policing Plan (Figure 2.0).

Figure 1.0 Information Management Strategy alignment with Force Strategic Plan

Figure 2.0 – Procedures/Policy Structure from Force Information Security Policy



4. INFORMATION MANAGEMENT VALUES

Although the IMS covers all information held by the force, it is primarily concerned with Police information. Police information is information required for a policing purpose, defined by APP, as necessary for:

- Protecting life and property
- Preserving order

- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility arising from common law or statute law

These five policing purposes provide the legal basis for the collecting, recording, evaluating, sharing and retaining of police information. To help achieve our policing objectives, this strategy has been developed to support the implementation of business change though the development of appropriate technology and business processes.

To achieve its objectives the Force will be guided by the following values of information management.

4.1 The Standards:

- Requirement for information to comply with the principles of the National Intelligence Model (NIM)
- Classification, grading and recording of police information (APP)
- Data Protection Act 2018
- NPCC Community Security Policy
- Eradication of unnecessary duplication
- Quality of information
- Evaluation
- Audit
- Risk management
- Vetting

4.2 Business Management:

- Duty to obtain and manage information;
- Compliance with the National Intelligence Model (NIM);
- Cost-effectiveness in information management;
- Commitment to an information culture;
- Information as a business asset - recognising the value of information used in decision making

4.3 People Management:

- Ownership of information;
- Users' responsibilities for information;
- Competency in handling information;
- Investment in appropriate resources, skills and training

4.4 Information Sharing:

- Duty to share information lawfully;
- The right information for the right person at the right time;
- Protection of sensitive information and sources;
- Obligations of those receiving information;

4.5 Data/Information Management:

- Review, retention and disposal of information;
- Conformity/compliance with external requirements;
- Use of appropriate information technology;
- Security of information;
- Storage of information;
- Data Protection Act 2018;

- Freedom of Information Act 2000
- NPCC Community Security Policy
- Criminal Procedures and Investigation Act 1996

5. SCOPE OF STRATEGY

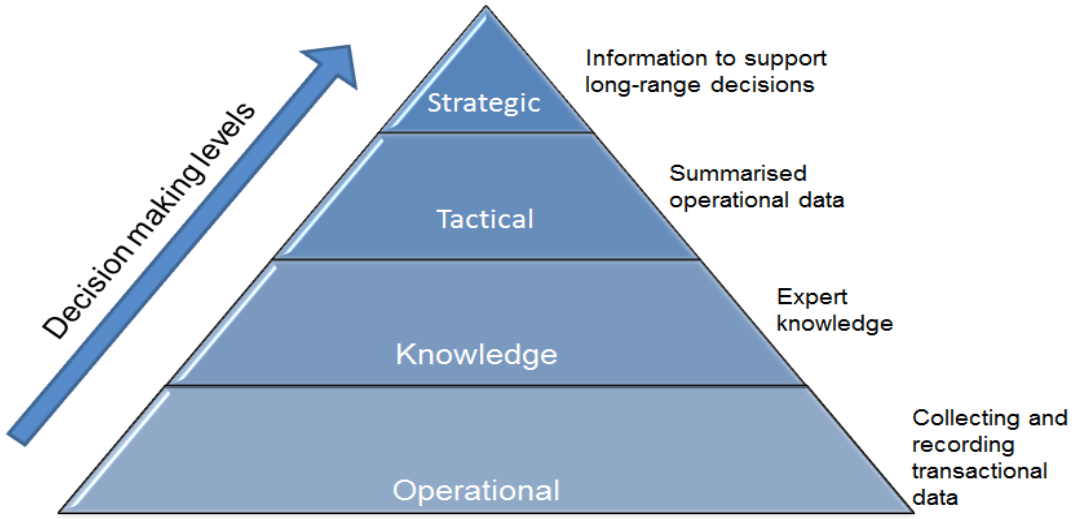
This IMS applies to all operational information processed by all staff employed by the North Wales Police in the course of carrying out their duties; this includes agencies, contractors and partners involved with police information. This strategy applies to all formats of information including electronic, digital, audio-visual and hard copy.

This strategy does not redefine organisational structures, nor determine technology-based solutions; however, it will inform future technical developments.

6. EXPLOITATION OF INFORMATION

North Wales Police will continue to build new capabilities to exploit the information resources we already have by interfacing silo data storage systems, aligning related information together and through improved analysis of records information.

Figure 3.0 North Wales Police utilises this model for information exploitation.



Within North Wales Police transactional data is used to run the operational day-day business; but critically it is also a key enabler for effective and timely decision making at all levels through the organisation.

The Anthony Triangle is an organizational model. Anthony's triangle takes a hierarchical view of management structure. With many operational decisions at the bottom, some tactical decisions in the middle and few but important strategic decisions at the top of the triangle. The higher in the triangle an item is, the more scope it covers and less precise it becomes. As items move down they become more detailed and apply more precisely.

7. STRATEGIC OBJECTIVES

North Wales Police collect and hold information for the policing purpose as defined within Authorised Professional Practice, and the Notification to the Information Commissioner.

In respect of its information management, North Wales Police is committed to complying with the Data Protection Act 2018, the NPCC/S Information Systems Community Security Policy (NPCC/S CSP) and to following five information management principles as defined by the International Standards Organisation (ISO) 15489:

i) to recognise and understand all types of information;
ii) to understand the legal issues and execute duty of care responsibilities;
iii) to identify and specify business processes and procedures;
iv) to identify enabling technologies to support business processes and procedures
v) to monitor and audit business processes and procedures.

To achieve its aim, North Wales Police will:

- ensure that the Force infrastructure and processes can provide the right information to the right people at the right time for the right purpose.

- ensure that staff are adequately trained in the ways that data protection and information security affects them in their role.

- ensure that information processed by North Wales Police has appropriate technical and organisational security to ensure its confidentiality, integrity, and availability to protect it from compromise, internal and external technical and non-technical threats.

- achieve a balance between the ease of appropriate and authorised access to the right information and appropriate security controls, through an information risk management process. This process will take account of the corporate and/or individual policing need and business requirement(s) when applying a combination of technical, procedural, physical and personnel controls to achieve a minimum residual risk.

- ascertain the adequacy of the security controls and the protection of personal data against unauthorised or unlawful processing, accidental loss, damage or destruction, by a combination of auditing, transaction monitoring, security reviews and other protective monitoring controls.

- have a fair and transparent process which allows North Wales Police to vigorously address any contravention by its staff, of its information processing policies.

- recognise information as a Force asset, have regard to Authorised Professional Practice, and link in with other legislation, statute and common law, regulations or national and local policies and procedures affecting the Force.

- manage its information in accordance with corporate standards; adopting the Force Information Standards Policy (FISP) and its underpinning procedures, in order to achieve this.

- support business processes by taking a coordinated and cohesive approach to information management to improve North Wales Police performance in support of the Force objectives.

- identify and support effective practice in the management of police information across all business areas; in conjunction with all other information management related policies, procedures and processes.

- promote a Force-wide integrated information lifecycle.

8. ROLES AND RESPONSIBILITIES FOR STRATEGIC INFORMATION MANAGEMENT

Chief Constable –Controller

North Wales Police has a corporate responsibility to own and manage all information processed for a policing purpose in accordance with the regulatory environment. The person with overall responsibility for this strategy is the Chief Constable who is also the Data Controller.

Director of Finance & Resources - Senior Information Risk Owner (SIRO)

The Director of Finance & Resources has the responsibility as the SIRO on behalf of North Wales Police. The SIRO has responsibility for both ensuring that information risk management processes (including the undertaking of risk assessments where appropriate) are established and adhered to, and for responding to any issues or risks that could adversely affect strategic goals or operational activities arising out of failures of primary or supporting information and records systems or processes.

The SIRO also has responsibility for signing the annual self-certification Community Security Policy (CSP) Compliance Matrix for submission to the Police Information Assurance Board, stating that they are aware of all residual risks relating to Force compliance with the CSP, and that they are satisfied with the current position.

It is the SIRO's responsibility to approve the Force's Risk Appetite.

Chief Information Officer

Chief Information Officer (CIO) within North Wales Police has central oversight of information held by the force. The CIO within North Wales Police will:

Approve the disposition of physical archives of records where there is a business requirement to split an archive of Group 1 or 2 records of like type between two or more separate locations.

Manage the Information Management Strategy and provide for it to be accessible on demand.

Provide guidance, encouragement and advice to ensure that this IMS is delivered and adhered to throughout the force.

Chair the Forces Information Security Board (ISB) and report as required to the SIRO and or Strategic Change and Collaboration Board.

Authorise the auditing of information systems, and the carrying out of audit processes within the Force.

Approve and authorise the:

- Force's Records Management Strategy
- Force's Records Management Policy
- Force's Retention Schedule
- Force's Records Off-Site Storage Policy
- Force's Review, Retention and Disposal Policy
- Force's Information Sharing Policy

- Force's FOI responses as required

Approve and authorise the disposal or destruction of information records, for all APP Review Groups.

Where appropriate, for example in relation to police information concerning sexual or violent offenders, destruction of records should also be approved by the Director of Intelligence, SIRO or ACC (via Operations Committee).
The CIO will ensure that Information Asset Owners (IAO's) are nominated for all information systems used to store or process police information.

Business Services, via Technology will provide an adequate IT, communications and business service to support this strategy. This will include appropriate technical, business and other related measures, with supporting documentation, to ensure confidentiality, integrity, availability and non-repudiation of information.

Each business area will have a named Information Asset Owner for their IT and information systems, who will be responsible for its creation, accuracy and its physical safekeeping.

IAO's will ensure that adequate security and data protection controls exist to appropriately protect information assets and the information held on the IT and information system(s) they have responsibility for. All processing of such information must comply with the Force Information Security Policy and its underpinning policy and procedures. These controls must include a Information Risk Assurance Report (IRAR) for each mission critical IT system and for each Police system, or a System Security Policy and Security Operating Procedures for any other system within their remit.

Everyone working for, or with the Force must understand and fulfil their responsibilities under this strategy.

9. OPERATIONAL CONSIDERATIONS

There are many operational issues which robust Information Management facilitates:

- Ability to find information easily
- Ability to share information easily both internally & externally
- Accountability, through legally admissible records
- Clear ownership of information
- Officer/Staff safety – using wrong, incomplete, old or missing information
- Consistency of information used
- Corporate memory – what has happened in the past
- Decision making
- Educating staff on what information we have
- Identifying redundant processes and information
- Knowing what our "customers" need and/or are entitled to
- Lack of space – paper records
- Meeting legal requirements and Government targets
- Partnership working
- Quality of Information used
- Reduced costs through removing duplicate information
- Reduction in the risk of losing information
- Removing unnecessary work – Reducing Burden
- Informing Information Management training requirements

10. FORCE POLICY DECISIONS FOR INFORMATION MANAGEMENT

1. The North Wales Police Information Management Strategy was adopted by the Force Change Committee on 27 July 2012. It was revised following adoption of the GDPR in May 2018 (Data Protection Act 2018).

2. North Wales Police has adopted and will comply with the national NPCCs Information Systems Community Security Policy (NPCC/s CSP). The Senior Information Risk Owner is the Director for Finance and Resources. The role of a Chief Information Officer role exists at a senior level within North Wales Police.

3. North Wales Police have adopted a Protective Marking Scheme based on the Government Security Classification.

4. North Wales Police will process personal data in compliance with the Data Protection Act 2018. The Chief Constable is the Controller for North Wales Police. Compliance measures will link in with other legislation, statute and common law.

5. An Information Security Board (ISB), chaired by the Chief Information Officer (CIO) will oversee information security and provide clear direction and visible management support for security initiatives.

6. Heads of Services and Departments will be responsible for complying with and implementing this policy and its procedures, within their own areas, in respect of the information asset and IT systems they have responsibility for, complying with and taking account of information security risk based decisions made by the CIO and the SIRO. They are responsible for adherence by their staff.

7. The National Intelligence Model will be used to assist in the identification of threats and vulnerabilities to the security of information processed by North Wales Police.

8. North Wales Police will comply with the Freedom of Information Act 2000.

9. Data Protection compliance and the security of our information assets will be achieved both proactively and reactively by implementing an appropriate combination of personnel, physical, procedural and technical controls. These will include: policies, procedures, protocols, risk assessments, tactical assessments, gap analysis, audit & monitoring, training & awareness, advice & guidance, organisational structures & responsibilities, software functions and consultation with business & information owners.

10. North Wales Police will have regard to the guidance within Authorised Professional Practice.

11. It will be the responsibility of all Police Officers and Police Staff to adhere to this policy and its procedures. The procedures which will support this policy will include an acceptable use section for all Employees. Non-compliance by staff, with the policy and its supporting procedures, could result in disciplinary findings of gross misconduct and/or criminal action which could lead to loss of employment. Please also see further clarity at point 23.

12. All staff will receive awareness training in the general principles of data protection and information security.

13. Staff are authorised to access and use information (to include personal data) held by North Wales Police for their role-related work purposes only. Staff must not use, or permit use of; any North Wales Police held information for private or non-work related use. Staff need to be aware that the unlawful obtaining or disclosure of personal data or the selling of that data, is an offence. See also point 23.

14. Only North Wales Police owned and authorised computers, laptops and other mobile devices and media may be used to process North Wales Police information. The movement of bulk data from one system to another or to another device or to another agency must be supported by a full risk assessment and authorised by the Chief Information Officer.

15. North Wales Police will record security incidents and vulnerabilities via the information Security Incident Procedure. In addition to the immediate steps detailed in the aforementioned procedure, vulnerabilities and threats to information security will be brought to the attention of the Chief Information Officer for consideration, monitoring and resolution to ensure any residual risk is acceptable and manageable.

16. Disaster Recovery and business continuity plans will be documented, implemented and regularly tested.

17. Information Sharing and Data Processing Agreements will be used to assist the business and to protect North Wales Police information.

18. The use of mobile data devices will take account of the business need and the prevailing threats.

19. North Wales Police will adopt ITIL (IT Infrastructure Library Best Practice) for its mission critical systems and its network and will have a program of work in place to implement this.

20. Although some devolvement of responsibilities has taken place within North Wales Police, the importance of Data Protection and Information Security standards remaining consistent throughout the Force is recognised in order to: -

    - maintain public confidence in the way North Wales Police process personal data and operate securely
    - protect our operational need to process personal data
    - ensure corporate compliance with relevant legislation, national policy and Codes of Connection e.g. Criminal Justice Extranet (CJX), PNC (Police National Computer), Airwave etc; to do otherwise would be likely to result in disconnection from police national systems
    - minimise the risks to the core information systems and the information they contain
    - maintain core and common work standards in order to minimise staff misunderstanding through, for example, role change, thereby minimising risks potentially created through staff movement across the Force.

21. Periodic reviews of security and Data Protection and information security risks, implemented controls and compliance with policy, will take place to:

    - Take account of changes to business requirements and priorities
    - Take account of changes in legislation
    - Consider new threats and vulnerabilities plus any changes in likelihood
    - Confirm controls remain effective and appropriate

22. Compliance with this policy will be measured through audit and monitoring procedures.

23. Where data protection and/or information security force policy (including all supporting procedures) have been breached, this will be assessed by Professional Standards Department to determine a proportionate response which may result in Gross Misconduct or Misconduct procedures. This assessment will be made on a case by case basis and will include consideration of all relevant factors including:

    - the merits of each individual case
    - the seriousness of the breach/amount or type of personal data or information
    - motive
    - other factors such as associated breaches/offences
    - impact of the breach on NWP, individuals and/or the public – potential or otherwise
    - wider public interest

    As each assessment will be individual it is not possible to specify breaches against outcome, however some examples are provided which would be likely to be assessed as Gross Misconduct: Note. this would also be a criminal offence.

    Unlawful obtaining, disclosing or sale of personal data;

    Where those working for, or on behalf of, North Wales Police have authority to obtain and disclose personal data in the course of their duties, they will commit section 170 offences if they use their position to obtain, disclose, or procure disclosure of personal data for their own purposes.

11. LEGAL REQUIREMENTS

- The Data Protection Act 2018;
- The Regulation of Investigatory Powers Act 2000;
- The Human Rights Act 1998;
- The Freedom of Information Act 2000;
- The Environmental Information Regulations 2004
- Authorised Professional Practice
- The Computer Misuse Act 1990.
- Police and Justice Act 2006
- Official Secrets Act 1989
- Police and Criminal Evidence Act 1984
- Police Act 1997
- Criminal Procedures and Investigations Act 1996
- Civil Contingencies Act 2004

- Police Reform and Social Responsibility Act 2011
- Crime and Disorder Act 2018
- Health and Safety at Work Act 1974
- The Copyright Designs and Patents Act 1988
- Bribery Act 2010

This strategy has been audited for compliance and compatibility with the Human Rights Act 1998 and the principles contained within it. Every effort has been made to ensure compliance and compatibility with the Act by applying the NPCC Human Rights Audit Tool-kit to the audit process.

At the time of ratifying this strategy the owner was satisfied that this document is compliant with all relevant legislation, including Human Rights, Race Relations, Data Protection, Equal Opportunities, Health & Safety and Disabilities legislation.