Heddlu Police
DYFED-POWYS

Information Sharing Policy

Policy summary:	***To give a clear understanding of the need to share information and provide a consistent approach to information sharing. To distinguish between the Force statutory obligations for sharing information and the need to share for immediate operational requirements and the safeguarding of adults and children.***
Policy number:	***012/2021***
Version control:	***Version: 5.0*** ***Date:*** *09/09/2021* ***Author:*** [redacted] ***Rationale:*** *New template and review* ***Full version control is included at the end of the policy***
Date implemented:	***09/09/2021***
Review date:	***09/09/2023*** ***The policy owner may undertake a review sooner if, for example, there are major changes to legislation associated with the policy, major changes to process, etc.***
Owner/contact:	***Information Sharing Officers, IMBA***
Approval	***Board: Information Assurance Board*** ***Date of approval: 09/09/2021***
Final Approval	***Board: Information Assurance Board*** ***Date of approval: 09/09/2021***
Consultation and approval	***This is a review and update to an existing policy onto a new template. The following have been consulted:*** ***Information Manager, Data Protection Officer, Data Protection Advisor***
Welsh Translation	***Yes***

1. Statement of Policy

This policy will ensure that Dyfed-Powys Police meets and implements the legal requirements under the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation 2018 (UK GDPR) and the Human Rights Act 1998 (HRA) when sharing personal information.

In order to assist in ensuring compliance, Dyfed-Powys Police will follow the College of Policing Authorised Professional Practice (APP) on Information Management – Information Sharing. Additionally Dyfed-Powys Police will follow guidance provided by the Information Commissioner's Office (ICO) which includes the ICO Data Sharing Code of Practice.

Dyfed-Powys Police will adhere to the College of Policing APP and the Wales Accord on the Sharing of Personal Information (WASPI), as the basis for guidance and templates for the development and creation of information sharing agreements.

***Applies (but not limited) to**: All categories of Dyfed-Powys Police employees, whether full-time, part-time, permanent, fixed term, temporary (including agency staff, associates and contractors) or seconded staff. Any employee accessing and using Force assets and property must have due regard to the contents of this policy.*

2. Policy Scope

Information is a vital asset to the organisation. Every department and individual uses information on a daily basis in order to fulfil the requirements of their role. This resource has to be managed and used appropriately to ensure Dyfed-Powys Police (DPP) is effective and efficient in meeting its responsibility for policing purposes and its statutory obligations. A policing purpose is defined as:

I. protecting life and property;
II. preserving order;
III. preventing the commission of offences;
IV. bringing offenders to justice;
V. any duty or responsibility arising from common or statute law.

Heddlu Police
DYFED-POWYS

Data provided within a Data Protection Impact Assessment (DPIA) may be used to identify privacy risks associated with the sharing of personal information.

DPP is committed to working in a joined-up manner with partner agencies to tackle issues relating to policing, protecting the public, crime and anti-social behaviour.

Effective information sharing facilitates good relations within the police service, with partner agencies, third parties, other organisations and the communities of the Dyfed-Powys Police area.

Information sharing between DPP and third parties is encouraged, but to safeguard the information and the subject of the information, there must be a formalised information sharing agreement (ISA) in place where regular sharing of information is taking place. The exceptions to this relate to emergency circumstances (more details below) or where non-regular sharing is taking place but there is a lawful basis engaged to cover the sharing. Advice regarding lawful basis can be obtained from the Information Management and Compliance Department whereone off sharing is taking place. DPP is a signatory to the Wales Accord on the Sharing of Personal Information (WASPI) and will pay due regard to the Accord and relevant guidance. Any ISAs will follow the WASPI template(s).

In emergency situations, Data Protection legislation allows the disclosure of personal data if it is in "*the vital interests*" of any person. DPP will ensure that in these circumstances information is shared promptly and effectively. This section covers exceptional, one-off disclosures of data in unexpected or emergency situations, for example, in cases of life or death, such as where an individual's identity and/or medical history is disclosed to a hospital's A&E department treating them, after a serious road accident. Disclosure should only take place when there are conditions of real urgency that necessitate the immediate sharing of data without reference to written guidelines and/or agreements. The rationale for sharing the information should be recorded.

Information sharing will only take place within the appropriate statutory and common law framework. Proper regard shall be paid to Data Protection legislation, the Human Rights Act 1998 and the common law duty of confidence.

All staff will be provided with the appropriate guidance with regard to the sharing of information with other agencies, to ensure that realistic expectations prevail and that common standards are applied across the organisations to address compliance with

the Data Protection principles. Everyone is responsible for ensuring that when information is shared, it is done so lawfully and proportionately and that the instances of information sharing and the rationale for the sharing are recorded.

The ICO (Information Commissioners Office) are the independent supervisory authority for data protection in the UK and uphold information rights for the public. Any breaches of data under the UK GDPR or DPA may be enforced by them with the powers they hold, as set out in Part 6 of the DPA 2018. This may, for example include warnings, fines or penalty notices. For serious breaches, fines of up to £17.5 million may be imposed.

Guidance on the types of agreements that may be used is available within the Information Sharing intranet page.

3. Powers and Policy/Legal Requirements

Dyfed-Powys Police has a legal obligation to comply with the UK General Data Protection Regulations (UK GDPR). The processing of personal data for law enforcement purposes is covered by the Law Enforcement Directive. Dyfed-Powys Police will refer to the College of Policing, APP - Information Management – Information Sharing, the ICO Code of Practice on Information Sharing and WASPI in the preparation of information sharing agreements.

Relevant legislation:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Freedom of Information Act 2000

Other Policy, Code of Practice and Guidance Documents:

- Article 29 Working Party (now the European Data Protection Board (EDPB)).
- Dyfed-Powys Police Data Protection Impact Assessment guidance document
- Dyfed-Powys Police Records Management Policy
- Dyfed-Powys Police Data Protection Policy

- Dyfed Powys Police Data Protection Breach Policy
- College of Policing APP – Information Management – Information Sharing
- ACPO Guide to Police Service Publication Scheme Compliance v4.0 (ACPO Minimum Requirements)
- ICO Data sharing: a code of practice
- ICO Data Sharing Information hub
- ICO Data Protection Impact Assessments Guidance
- International Standard on Records Management, ISO 15489
- The Wales Accord on the Sharing of Personal Information (WASPI)

In addition, certain data will be subject to other legislation covering particular subject areas. Departments should ensure that they are aware of the legislation governing their work and its bearing on data sharing.

EQUALITY IMPACT ASSESSMENT

Section 4 of the Equality Act 2010 sets out the **protected characteristics** that qualify for protection under the Act as follows: Age; Disability; Gender Reassignment; Marriage and Civil Partnership; Pregnancy and Maternity; Race; Religion or Belief; Sex; Sexual Orientation.

The **public sector equality duty** places a proactive legal requirement on public bodies to have regard, in the exercise of their functions, to the need to:

- eliminate discrimination, harassment, victimisation, and any other conduct that is unlawful under the Act;
- advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;
- foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

The equality duty applies to all protected characteristics with the exception of Marriage and Civil Partnership, to which only the duty to have regard to the need to eliminate discrimination applies.

Carrying out an **equality impact assessment** involves systematically assessing the likely or actual effects of policies on people in respect of all the protected characteristics set out above.

Heddlu Police
DYFED-POWYS

An equality impact assessment should be carried out on any policy that is **relevant** to the public sector equality duty. An equality impact assessment template is available here.

Equality Impact Assessment Completed

Name:	[redacted]
Department:	Information Management and Compliance
Signed:	[redacted]
Date:	19 August 2021

HUMAN RIGHTS ACT CERTIFICATE OF COMPLIANCE

This policy has been drafted in accordance with the Human Rights Act and has been reviewed on the basis of its content and the supporting evidence and it is deemed compliant with that Act and the principles underpinning it.

Name:	[redacted]
Department:	Legal Services
Signed:	[redacted]
Date:	19.08.2021

Heddlu Police
DYFED-POWYS

4. Options and Contingencies

Roles and Responsibilities within Dyfed-Powys Police

Chief Constable: The Chief Constable of Dyfed-Powys Police is the Data Controller and as such has overall responsibility for the lawful processing of all personal data processed by the Force. They also have overall accountability for procedural documents and have ultimate responsibility for compliance of this policy and data protection across the entire Force

Senior Information Risk Owner (SIRO): The Deputy Chief Constable (DCC) of Dyfed-Powys Police is the appointed Senior Information Risk Owner (SIRO). They are responsible for:

- Overall accountability for information risk across the Force
- Representing and championing information risk
- Remaining up-to-date on all necessary training in order to remain effective in their role as SIRO
- Understanding the impact of information risks on the Force's risk register, and how those risks may be minimised and managed, and
- Chairing the Information Assurance Board

Data Protection Officer (DPO): The Head of Information Management of Dyfed-Powys Police is the appointed Data Protection Officer (DPO). They are responsible for:

- Protecting the confidentiality of personal data across the Force
- Representing and championing data protection issues and requirements
- Ensuring that the Force satisfies the highest practical standards for handling personal data
- Enabling suitable information sharing with other bodies
- Ensuring that data protection issues are appropriately reflected in Force policies, procedures, processes and strategies for employees
- Assisting the Force in demonstrating compliance with UK data protection legislation as part of the enhanced focus on accountability
- Acting as a point of contact for data subjects and the ICO, and
- Informing and advising on data protection obligations Force wide.

Information Asset Owner(s): Information Asset Owners (IAO) are senior employees who are the nominated owners of one or more identified information assets. They are responsible for:

- Ensuring that the information assets that they have responsibility for are appropriately protected and any information sharing undertaken is shared appropriately, in line with legislation and any relevant information sharing protocols which are in place.
- IAO's are responsible for ensuring that appropriate information sharing protocols are in place where regular sharing of information is taking place between the Force and partner agencies.
- IAO's are responsible for ensuring that early engagement with the Information Management and Compliance Department takes place where new information sharing activities are being considered.
- Monitoring and understanding what information – paper and electronic – is being held and how it is maintained; knowing and approving who has access to it and why.
- Seeking to use information fully within the law
- Identifying and addressing risks to the information, and
- Encouraging a culture that values, protects and uses information for the public good.

Disclosure, Records and FOI Manager: The Disclosure, Records and FOI Manager has responsibility for the oversight of the preparation of information sharing protocols. They are responsible for:

- To effectively direct, control, monitor and provide management oversight of the activities carried out by information sharing officers in order to ensure compliance.
- Ensuring that information sharing staff have the relevant, support, skills and competencies required to undertake their role and ensuring that they have a good understanding of their role and responsibilities with the aim of providing an effective service in compliance with relevant legislation, guidance, policy etc.
- Provide specialist advice on information sharing matters to staff across the Force

- Establish procedures and safeguards to manage the Chief Officer's statutory obligations in respect to the disclosure of information under information compliance legislation.

Information Sharing Officers: Information Sharing Officers are responsible for:

- The co-ordination and preparation of all information sharing protocols, data processing contracts, data disclosure agreements and associated documents.
- To administer and co-ordinate the data protection impact assessment process within the Force.
- Through proactively working with Force departments and Basic Command Units (BCUs) establish where information sharing and information disclosure is taking place and ensure that, where necessary, data protection impact assessments have been undertaken and relevant agreements are in place
- To develop and sustain effective working relationships with Dyfed Powys Police staff, OPCC staff, partner agencies and other agencies.
- To provide specialist advice to colleagues, partner agencies and other agencies on correct protocols to follow in respect to information sharing, data disclosures and the data protection impact assessment process.
- To maintain a record of and manage agreements and accompanying documents in respect of all information sharing and data disclosures and data protection impact assessments for the Force.
- To support the Disclosure, Records and FOI Manager to implement and monitor all procedural changes necessitated by legislative changes.
- To keep up to date with developments and changes in relation to information sharing, information disclosure and data privacy and to keep abreast of national changes to Information Management and Compliance practices, changes to relevant legislation, Information Commissioner's Office Code of Practice and guidance and the Wales Accord on the Sharing of Personal Information (WASPI) in order to provide guidance and support to staff, officers and external customers in such matters

Data Protection Advisor: The Data Protection Advisor is responsible for:

- Providing Data Protection advice as part of the development of information sharing agreements to include advising on the legal basis for the sharing of personal information.
- Maintaining awareness of data protection issues across the Force
- Provide specialist advice on information sharing matters to staff across the Force
- Encouraging a culture that values, protects and uses information for the public good
- Ensuring all line managers are aware of their responsibilities and accountability regarding data protection.
- Ensuring all employees are provided with the appropriate and necessary training to further their understanding of the principles of data protection and their application, and
- Informing and advising on data protection obligations Force wide

Information Assurance Board: The role of the Board is:

- To maintain strategic oversight, and support the management of, all activities related to the use, processing, retention, and transmission of information or data under the control of Dyfed-Powys Police and the structures, systems and processes used for those purposes in accordance with the College of Policing APP on Information Management which includes the Act and the Regulations;
- Provide governance support and direction to the Information Management and Compliance Department in line with the Force vision to 'Safeguard our Communities Together'; and
- Work in line with the other groups and boards in delivering the mission, vision and values of the Force, the Chief Constable's vision and the delivery plan in support of the Police and Crime Plan.

Line Managers: All Line Managers are responsible for:

- Ensuring that the Information Sharing Policy is implemented and adhered to within their department.
- Ensuring that appropriate information sharing protocols are in place where regular sharing of information is taking place between the Force and partner agencies.

- Ensuring that early engagement with the Information Management and Compliance Department takes place where new information sharing activities are being considered.
- Ensuring that where information sharing is taking place that it is undertaken appropriately, in line with legislation and sharing activity is appropriately recorded.

All Employees: All employees have responsibility for**:**

- Ensuring that they are familiar with the Data Protection Act 2018 and take personal responsibility to secure data, keep it up to date and share only what is necessary in line with legislation, guidance, and with force policies and procedures.
- All employees are responsible for adhering to the Information Sharing Policy and related documentation.
- Ensuring that appropriate information sharing protocols are in place when considering sharing information with partner agencies, unless the sharing is deemed to be urgent, as identified above.
- Ensuring that where information sharing is taking place that it is undertaken appropriately, in line with legislation and sharing activity is appropriately recorded.
- Ensure that only the minimum necessary amount of information will be shared

Code of Ethics

In line with the nine Policing Principles of the Code of Ethics, this Policy seeks to address the following:-

- **Accountability** - You are answerable for your decisions, actions and omissions.
- **Fairness** - You treat people fairly.
- **Honesty** - You are truthful and trustworthy.
- **Integrity** - You always do the right thing.
- **Leadership** - You lead by good example.
- **Objectivity** - You make choices on evidence and your best professional judgement.

- **Openness** - You are open and transparent in your actions and decisions.
- **Respect** - You treat everyone with respect.
- **Selflessness** - You act in the public interest.

This policy places specific emphasis on:

Accountability - Under UK data protection legislation, the accountability principle requires taking responsibility for how personal data is dealt with and proving compliance with the other data protection principles.

Fairness - Under UK data protection legislation, the element of fairness (which forms part of a larger principle) requires the processing of personal data to always be fair as well as lawful. This means not using personal data in ways that could have unjustified adverse effects on the data subject.

CODE OF ETHICS CERTIFICATE OF COMPLIANCE
This policy has been drafted in accordance with the Code of Ethics and has been reviewed on the basis of its content and the supporting evidence and it is deemed compliant with that Code and the principles underpinning it.

Name:	[redacted]
Department:	Information Management and Compliance
Signed:	[redacted]
Date:	19 August 2021

5. Take action and review

The SIRO, DPO and Information Assurance board will be kept informed of the Information Sharing agreements in place.

This policy is owned by the Information Management and Compliance Department. The review process will be conducted by the Information Sharing officer under the

direction of the Disclosure, Records and FOI Manager every two years to ensure the continued effectiveness of the policy, and taking into account any changes to legislation, national guidance, ICO guidance, etc., unless changes before this period indicate that this policy requires updating.

The effectiveness of the policy will be monitored regularly within the two year review period and any major concerns will be escalated as appropriate. Information sharing agreements will be subject to auditing to ensure the effectiveness of the provision of Information Sharing Agreements in line with this policy.

In the case of any queries regarding this policy, its content, or associated guidance documentation - individuals should contact Dyfed-Powys Police Information Sharing Officers or the Disclosure Records and FOI Manager.

Appropriate promotion of this policy will take place which can include awareness raising when training inputs and presentations are provided to staff across the Force. The policy will be made available on the Force Intranet and Internet.

Where there are issues identified, the Information Sharing Officer(s) or the Disclosure, Records and FOI Manager will work closely with representatives from the relevant departments to address the issues and ensure that lessons are learned.

Any issues of concern or risk in respect to compliance with the sharing of information will be escalated to the Data Protection Officer, Data Protection Advisor, Force Information Security Officer, Force SIRO and Information Assurance Board, dependent on severity. Where it is established that a Data breach has occurred as a result of the sharing of information the Force Data Protection Breach Policy and associated data breach reporting process will be followed. Such reporting, and subsequent investigation, may highlight issues with this policy, the information sharing process, information sharing protocols and associated guidance, which could result in a necessary review. If this is the case, relevant action will be taken. The Disclosure, records and FOI Manager will work closely with representatives from the relevant departments and the Data Protection Advisor to address the issues and ensure that any lessons learned will be fully reported and cascaded as necessary.

Key Performance Indicators: Statistics in relation to past, current and future agreements will be reported monthly to the Data Protection Officer and quarterly to the Information Assurance board.

Heddlu Police
DYFED-POWYS

Freedom of Information Act 2000

Section 19 of the Freedom of Information Act 2000 places a requirement upon the Force to publish all policies on the Force website. Policies are why we do things and procedures are how we do them. A case-by-case review of procedures must be undertaken to protect law enforcement and health and safety considerations. Where a combined policy and procedure document is being produced the Force is legally required to publish the policy section and assess the procedure part to ensure no sensitive information is published. Generally the default position shall be that a policy and accompanying procedure document will be produced separately.

There is a requirement therefore to review this document to establish its suitability for publication. Please identify below whether the document is suitable for publication in its entirety or not. Where it is believed that disclosure will be harmful please articulate the harm that publication would cause and highlight the relevant sections within the document. Where it is perceived that there is harm in disclosure the document should be forwarded to the Disclosure Unit for review.

Suitability for publication

Suitability for publication	**Yes/No**	**Date**	**Signature**
Document is suitable for publication in its entirety	Yes	19.08.21	[redacted]
Document is suitable for publication in part, I have identified those sections which I believe are not suitable for disclosure and have articulated below the harm which would be caused by publication.	N/A		

Harm in publication: N/A

FOI review – to be completed by Disclosure Unit

(Only required if author believes there is any harm in disclosure)

Suitability for publication	Yes/No	Date	FOI Decision Maker
Document is suitable for publication in its entirety			
Document is suitable for disclosure in part and relevant redactions have been applied. A public facing version has been created.			

Once review has been undertaken FOI Disclosure Officer to return document to policy author and following sign–off document to be published within Force Publication Scheme. Any future changes to the document should be brought to the attention of the Disclosure Unit, as appropriate.

Heddlu Police
DYFED-POWYS

FULL VERSION CONTROL

Version	Date	Author	Rationale
5.0	09/09/2021	[redacted]	Sign-off – new template and review
4.0	19/05/2015	[redacted]	Changes to reflect changes to Force Structure following completion of Public First
3.0	16/08/2013		Rewrite policy to reflect launch of Authorised Professional Practice (Decision Making)
2.0	16/07/2013		Revision to reflect change in departmental structure
1.0	21/12/2011		First version