Heddlu Police
DYFED-POWYS

Data Protection Impact Assessment Policy

Policy summary:	***The Data Protection Impact Assessment Policy enables Dyfed-Powys Police to establish good practices around the use and handling of information, promote a culture of awareness and improvement and comply with legislation. Its aim is to provide employees with a framework that outlines the appropriate process for managing projects that process personal data, in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018 and other related legislation.***
Policy number:	***015/2021***
Version control:	***Version: 3.0*** ***Date:*** *November 2021* ***Author:*** [redacted] ***Rationale:*** *Role change in point 4* ***A full version control is available here.***
Date implemented:	**April 2021**
Review date:	**April 2023**
Owner/contact:	***Data Protection Advisor***
Approval	**Approval:** Information Manager/Data Protection Officer (DPO authorised to approve IMBA policies at IAB of 16/12/20). **Date of approval:** 09 April 2021
Consultation and approval	***Information Management and Compliance*** ***Legal Services***
Welsh Translation	***Yes***

1. Statement of Policy

The Data Protection Impact Assessment Policy enables Dyfed-Powys Police to establish good practices around the use and handling of information, promote a culture of awareness and improvement and comply with legislation. Its aim is to provide employees with a framework that outlines the appropriate process for managing projects that process personal data, in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018 and other related legislation.

The Information Commissioner's Office (ICO) defines a Data Protection Impact Assessment (DPIA) as a process to help an organisation identify and minimise the data protection risks of a project. One must be completed for processing that is **likely to result in a high risk** to individuals, or any major, new project or initiative involving the use of personal data.

This policy is essential in helping Dyfed-Powys Police employees understand the correct process for managing projects and initiatives that process personal data. Information is a powerful tool and a vital asset, in regard to both law enforcement processing and the management of services and resources across the Force. It is of paramount importance that employees understand how to handle personal data lawfully and that they understand their responsibilities when considering new methods of processing. This applies to information relating to the organisation, its employees and the public. It is also vital that appropriate policies, procedures and processes provide a solid foundation for data protection compliance across the entire Force.

***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.*

Heddlu Police
DYFED-POWYS

2. Policy Scope

Dyfed-Powys Police has a statutory obligation to process personal data in accordance with the provisions of the UK GDPR in respect of non law enforcement processing and the DPA 2018 in respect of law enforcement processing.

Under the UK GDPR Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95 there are legal requirements imposed on the Force in regard to the completion of DPIAs. The aim of this policy is to ensure consistency in Dyfed-Powys Police's management of any major, new projects or initiatives involving the use of personal data (even if there is no specific indication of likely high risk) and compliance with the relevant legislation and best practice guidance.

Dyfed-Powys Police complies with the College of Policing Authorised Professional Practice (APP) on Information Management. The APP provides clear standards and guidance in regards to privacy by design and default and DPIAs under UK data protection legislation. In addition, Dyfed-Powys Police follows any and all relevant guidance provided by the Information Commissioner's Office (ICO) in regard to data protection matters.

All employees are required to understand their responsibilities under UK data protection legislation, with specific staff groups requiring more detailed knowledge around DPIAs. Data protection is the responsibility of **ALL** employees and this policy must be adhered to. This policy is triggered as soon as a new project or initiative involving the use of personal data is identified, or there is a change to the nature, scope, context or purposes of processing underway in an existing project that involves personal data.

If this policy is not adhered to and/or DPIAs are not completed at the appropriate time, potential risks to the Force include, but are not limited to:

- Inability to secure and maintain individuals' trust and confidence in the Force, due to being unable to reassure individuals that their interests are being protected and insufficient attempts have been made to reduce any negative impact on them
- Damage to the Force reputation

- Failure to comply with relevant legislation, including demonstrating compliance with accountability obligations
- The potential breach of UK data protection legislation, resulting in potential action being taken against the Force by the ICO, for being unable to meet its information rights obligations
- Financial loss

3. Powers and Policy/Legal Requirements

Dyfed-Powys Police has a legal obligation to comply with UK data protection legislation. Dyfed-Powys Police will also refer to the College of Policing, APP - Information Management – Data Protection – Data protection impact assessment (DPIA).

Relevant legislation includes:

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

The requirement of completing DPIAs, by the Force, is governed by the UK GDPR. Key staff groups with any level of involvement in new projects and initiatives across the Force are required to understand their responsibilities under this legislation in regard to recognising when a DPIA is required, and knowing which department to contact for advice and guidance. This includes, but is not limited to, Information Asset Owners (IAO), Information Asset Administrators (IAA) and Project Managers. Further details are available in the DPIA Guidance document.

This policy should also be read in conjunction with the following related policies, protocols, practices and/or services agreements:

- DPIA Guidance Document
- DPIA Template Document
- Data Protection Policy
- Information Security Policy
- Freedom of Information Policy

- Information Sharing Policy
- Records Management Policy
- Data Protection Compliance Audit Policy
- College of Policing Authorised Professional Practice (APP) Information Management Guidance
- The National Police Chiefs Council (NPCC) Data Protection Manual of Guidance
- The Information Commissioner's Office's Code of Practice and Guidance

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.

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.

Heddlu Police
DYFED-POWYS

EQUALITY IMPACT ASSESSMENT COMPLETED

Name:	[redacted]
Department:	IMBA
Signed:	[redacted]
Date:	07/04/2021

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:	09/04/2021

4. Options and Contingencies

Roles and Responsibilities within Dyfed-Powys Police

4.1. 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.

4.2. 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
- Where necessary, providing sign-off for DPIAs, and
- Chairing the Information Assurance Board

4.3. 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, including that of DPIAs
- Ensuring that the Force satisfies the highest practical standards for handling personal data
- Enabling suitable information sharing with other bodies
- Ensuring that DPIAs 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 employees, data subjects and the ICO in regard to DPIAs
- Informing and advising on data protection obligations, in regard to DPIAs, Force wide
- Where necessary, stipulating a DPIA is required for a specific purpose
- Providing advice and guidance on the content of DPIAs, and
- Where necessary, consulting with the ICO in regard to high-risk processing identified within a DPIA.

4.4. Information Asset Owner(s) (IAO)

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

- 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
- Recognising when a DPIA is required, and knowing which departments should be consulted as part of that process and where to gain advice and guidance
- Completing DPIAs as early in a project schedule as possible
- Providing sign-off for completed DPIAs
- Reviewing DPIAs when necessary
- Seeking to use information fully within the law
- Identifying and addressing risks to the information
- Encouraging a culture that values, protects and uses information for the public good, and
- Ensuring that the Data Protection Impact Assessment Policy is implemented and adhered to within their area of business.

4.5. Data Protection Advisor

The Data Protection Advisor is responsible for:

- Maintaining awareness of data protection issues across the Force, including DPIA related matters
- Encouraging a culture that values, protects and uses information for the public good
- Reviewing and updating the Data Protection Impact Assessment Policy when appropriate, in line with legislation
- Reviewing and updating all procedures and processes relating to this policy where appropriate
- Ensuring all IAOs are aware of their responsibilities and accountability regarding DPIAs and the requirements of this policy
- Providing advice and guidance on the content of DPIAs
- Ensuring relevant employees are provided with the appropriate and necessary training to further their understanding of their responsibilities when considering new methods of processing, and
- Informing and advising on data protection obligations Force wide, including that of DPIAS.

4.6. Project Managers

Project Managers are responsible for:

- Recognising when a DPIA is required, and knowing which department to contact for advice and guidance
- Where necessary, assisting the IAO with completing DPIAs as early in a project schedule as possible

4.7. Corporate Governance Manager

The Corporate Governance Manager is responsible for:

- Providing advice and guidance on the content of DPIAs
- Reviewing areas of identified risk within DPIAs and assessing the identified mitigation and management controls. This brings an independent quality assurance function to the risks posed within the DPIA. This advice and guidance ensures the risk assessment within the DPIA is robust and fit for purpose

4.8. Information Security Officer

The Information Security Officer is responsible for:

- Providing advice and guidance on the content of DPIAs
- Ensuring that the Force Information Asset Register (IAR) is update to reflect any and all relevant information included in DPIAs

4.9. Information Sharing Officers

Information Sharing Officers are responsible for:

- Acting as a point of contact for employees in regard to DPIAs
- Where necessary, advising if a DPIA is required for a specific purpose
- Assisting IAOs/Project Managers in completing DPIAs by providing advice and guidance
- Remaining up-to-date on all DPIA advice and guidance from relevant sources e.g. the ICO
- Representing and championing the requirement of DPIAs across the Force
- Enabling suitable information sharing with other bodies
- Linking with subject matter experts within the Force to progress DPIAs
- Ensuring all relevant employees fulfill their responsibilities under a DPIA in a reasonable timeframe
- Where applicable, facilitating the publication of DPIAs, and
- Commencing the review of DPIA when necessary.

4.10. Data Protection Compliance Officer

The Data Protection Compliance Officer is responsible for:

- Ensuring all recommendations made during the DPIA process are satisfied, through regular contact with the IAO and conducting Data Protection Compliance Audits

4.11. All Employees

All employees are required to understand their responsibilities under UK data protection legislation, and to know to contact the Information Management Department with any DPIA related queries.

Code of Ethics principles

The Code of Ethics is a national code of practice, which defines core policing values and the standards of behaviour for everyone who works in policing. In line with these nine principles, the Data Protection Impact Assessment Policy seeks to embed 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. DPIAs are a key part of an organisations accountability obligations under the UK GDPR.
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 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:	IMBA
Signed:	[redacted]
Date:	07/04/2021

5. Take action and review

This policy is owned by the Information Management and Compliance Department. The review process will be conducted by the Data Protection Advisor on a biennial basis to ensure the continued effectiveness of the policy, and taking into account any changes to legislation, national guidance, ICO guidance etc.

The effectiveness of the policy will be monitored on a regular basis over and above the two year review period and any major concerns will be escalated as appropriate.

Effectiveness of the policy will be measured through the Force Data Protection Compliance Audit process and auditing the access to the document and associated guidance documentation. The aim being to check awareness of the need to complete DPIAs and ensuring compliance with UK data protection legislation. Also, measuring the number of queries directed at the Department in regard to the DPIA process and the policy will allow its effectiveness to be measured.

In the case of any queries regarding this policy, it's content, or associated guidance documentation - individuals should contact:

- Dyfed-Powys Police Data Protection Advisor
- Email: dataprotection@dyfed-powys.pnn.police.uk
- Post: Data Protection Advisor, Dyfed-Powys Police, PO BOX 99, Llangunnor, Carmarthenshire, SA31 2PF

Appropriate promotion of this policy will take place, which can include awareness raising when training inputs and presentations are provided to employees across the Force. The policy will be made available on the Force intranet and internet sites. Publication via the internet will ensure that it is available for public view.

Any issues of concern or risk in respect to compliance with UK data protection legislation across the Force will be escalated to the Force Data Protection Officer, Force SIRO and Information Assurance Board, dependent on severity.

Information regarding any other potential data protection issues across the Force, will be processed in line with the Force Data Protection Policy. Such reporting, and subsequent investigation, may highlight issues with this policy and associated guidance, which could result in a necessary review. If this is the case, relevant action will be taken. The Data Protection Advisor will work closely with representatives from the relevant departments to address the issues and ensure that any lessons learned will be fully reported and cascaded as necessary.

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	07/04/2021	[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.			

Outline of any harm identified in publication:

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
1.0	July 2018	[redacted]	New Policy
2.0	April 2021	[redacted]	New Policy Template
3.0	November 2021	[redacted]	Role change in point 4