Heddlu Police
DYFED-POWYS

Records Management Policy

Policy summary:	***The Records Management Policy is intended to establish compliance with law and published national guidance in respect of the secure retention, review and appropriate secure disposal of records and information collected during the course of policing business. The policy aims to provide a framework to manage records confidently that provides robust and systematic processes for managing records held in both paper and electronic format.***
Policy number:	**005/2021**
Version control:	***Version 7*** ***Review Date: October 2023*** ***A full version control is available here.***
Date implemented:	***04/02/2021***
Review date:	***October 2025***
Owner/contact:	***Records and Data Quality Supervisor*** ***Information Management Business Area***
Approval	***Board: Information Assurance Board*** ***Date of approval: December 2023***
Final Approval	***Board: Information Assurance Board*** ***Date of approval: December 2023***
Consultation and approval	**Heads of CID & CJD** **IMBA** **Data Protection** **FOI** **Legal Services**
Welsh Translation	***Yes***

1. Statement of Policy

Dyfed Powys Police recognises that the efficient management of its records is necessary to comply with its legal obligations. Information is a key asset to the police service. The effective management of information across all aspects of policing is vital to delivering the core priorities of the service, which are to protect the public and reduce crime. To carry out the functions of policing the Force has to process personal and organisational information from a range of sources and in a number of different forms.

The integrity of police information relies on the information being trusted, acceptable, useable and available. It should be in a format that is accessible and easy to use, whether it is an electronic, photographic or paper format.

The purpose of records management from policing and business perspectives is to ensure that information is recorded and maintained in such a way that its evidential weight and integrity is not compromised over time. To achieve this, records need to be managed throughout their lifecycle, from creation through to disposal.

1. Dyfed Powys Police acknowledge that personal data will only be retained for a valid policing purpose, and such data needs to be accurate and relevant.

Effective processes will be utilised to ensure that all such data is subject to periodic review where decisions can be documented justifying either the continued retention or deletion of such data.

2. Dyfed-Powys police will retain and manage all digital and paper records, in compliance with Data Protection laws and regulations. Organisational records will be retained in line with relevant legislation and guidance (e.g. National Archives).

3. Dyfed-Powys Police will use the Management of Police Information guidance on the common process, collection and recording, evaluation and retention, review and disposal of police information as contained within the College of Policing Authorised Professional Practice (APP) - Information Management, to inform its records management processes.

Dyfed-Powys Police will apply the framework for retention timescales set out in NPCC Retention Guidelines to determine such retention timescales.

However, we will remain cognisant of the principles of archiving in the public interest as set out in the Data Protection Act 2018 to ensure that records which may qualify for such longer retention (as defined by National Records Office) are retained for such public interest purposes.

All paper records containing personal information, which require retention, must be uploaded onto existing electronic systems, in order that records management processes can be applied to such records. Paper copies of records should only remain in existence while legal obligations for their retention (such as Criminal Procedures Investigations Act) apply. The Force Practice for 'Managing the review, retention & storage of documentation accumulated during Criminal Investigations' should be adhered to for such paper copies.

This will ensure that the Force is aware of what paper records are held. When records review/ retention/disposal processes are applied to retained records and any decision to delete records is taken, the process will be effective in clearing all copies of such personal information. Consequently, any decision to delete an electronic copy of a record does not result in the continued existence of a paper copy of the same record.

This policy, applies to the management of all organisational, operational and business records (whether containing personal data or not) in all technical or physical formats or media, collected, received, created, held, shared, disseminated, disclosed, maintained, reviewed, retained or disposed of by officers, staff and volunteers of Dyfed Powys Police and 3rd parties in the course of carrying out the functions of the organisation, whether recorded in the language of English or Welsh.

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

Heddlu Police
DYFED-POWYS

2.Policy Scope

Key drivers for this policy and the need for a consistent approach are legislative, particularly the principles of the Data Protection Act 2018, the requirements of the Code of Practice under Section 46 of the Freedom of Information Act and the College of Policing Authorised Professional Practice (APP) on Information Management. A failure to record, retain, review and dispose of information appropriately may constitute a breach and, ultimately, undermine public confidence in the Force.

ISO 15489 defines a record as "*information created, received, and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business*".

Due to the nature of policing it is essential to distinguish between information processed for a policing purpose and information required for business functions that support the service to be delivered.

Records created by the Force broadly fall into two categories:

- Organisational and administrative records (also referred to as corporate) – which contain information processed to enable the discharge of police services such as financial information, policies and procedures and information relating to employees.

- Police records – contain information processed for a policing purpose namely:

  protecting life and property
  preserving order
  preventing the commission of offences
  bringing offenders to justice, and
  any duty or responsibility of the police arising from common or statute law

It should be noted that the policing purpose definition is wider than the Part 3 Data Protection Act 2018 (DPA 2018) definition of law enforcement purpose, which is:

> *'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'.*

Consequently some information recorded for a policing purpose may be processed under Part 3 of the DPA 2018 and some under the UK General Data Protection Regulation (UK GDPR).

Heddlu Police
DYFED-POWYS

It is recognised that police records include data obtained both overtly and covertly (In accordance with authorisations approved under Regulation of Investigatory Powers Act 2000, and Investigatory Powers Act 2016). Such authorised data is managed through the Central Authorisations Bureau, and this policy applies equally to the management and retention/ disposal of such data.

The core principles for processing all types of information that becomes a record are the same for the two categories. However, the nature of information recorded for a policing purpose requires extra safeguards.

The purpose of this policy is to provide police personnel with guidance to assist the records management process, taking into account the requirements of relevant legislation and the rights of individuals whose information is recorded and retained and the requirements associated with organisational and corporate records held by the Force.

Personal Information: Application of MoPI Guidance to achieve legal compliance with Data Protection Law and regulations will ensure that personal data on individuals is retained not longer than that which is necessary for policing purposes, and members of the public can be confident that their data is being retained appropriately and securely.

Corporate Records: Corporate/organisational records will be retained in line with the NPCC National Guidance on the Minimum Standards for the Retention and Disposal of Police Records.

This policy will also ensure consistency across systems in respect of the retention and management of such records. Such processes will apply to all existing electronic systems including command and control, case management & intelligence, as well as records retained within internal communication systems including those within Microsoft Office 365.

The Policy will apply equally to data held within Cloud services, and deletion will include deletion from such remote storage facilities.

The Force will comply with APP guidance by ensuring information entered onto a record (paper or IT based) conforms to the following:

- Information is recorded for Law Enforcement Purposes

- Information is recorded in the appropriate format for the business area in which it is held.
- Information is recorded according to the data quality principles – accurate, adequate, relevant and timely
- Checks are made to avoid creating duplicate records.
- Links are made to existing records.
- Correct Government Security Classification (GSC) marking is used.

Compliance with APP guidance on record creation and local Data Quality standards is the responsibility of everyone who enters new data onto police databases. This important principle should be conveyed and reinforced in initial training and in subsequent practice.

It will be the line manager's responsibility to carry out regular dip samples to check that the information recorded is to the required standard. Where the standard is not being met, feedback should be given, and where necessary, appropriate training or guidance arranged using the Development Appraisal Process.

Each operational/business area will have in place clearly worded and effectively disseminated procedures, rules and conventions relating to each police system/process in that area. These procedures will take into account the legislative and regulatory environments in which the operational/business area works and include controls to ensure each record is created using the appropriate templates, forms or database.

Information received from other agencies will be treated and evaluated as a piece of intelligence.

Where guidance allows for automated processes to delete data following the expiry of 'clear periods' of time, it is acknowledged that such automation creates some risk of deletion of data which may later have been of value within Policing. Such automated processes will only be applied to information or subjects which are graded lower than Group 2 under MoPI guidance, which relates to matters NOT perceived as presenting significant risk of harm to communities.

Other Relevant Guidance:

- Storage & Retention of Paper Records resulting from Criminal Investigations Policy
- Freedom of Information Policy
- Data Protection Policy

- Information Security Policy and associated Standards
- Government Security Classification Policy
- Information Sharing Policy

3 Powers and Policy/Legal Requirements

Dyfed Powys Police will use the College of Policing, APP - Information Management when managing its records and will comply with the requirements of the Lord Chancellor's Code of Practice on the management of records issued under Section 46 of the Freedom of Information Act 2000.

Relevant Legislation:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Code of Practice under S46 of the Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Criminal Procedure and Investigations Act 1996
- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000
- Investigatory Powers Act 2016

Other Policy and Code of Practice

- College of Policing Authorised Professional Practice (APP) on Information Management
- Information Commissioner's Office Code of Practice on data sharing

4. Options and Contingencies

Governance

Responsibilities for Records Management

Heddlu Police
DYFED-POWYS

Good Records Management is a responsibility shared by all members of the Force but ultimate responsibility rests with the **Chief Constable as Data Controller.**

Chief Constable: As Data Controller the Chief Constable is the person who determines the purpose and means by which the processing of personal data occurs.

Senior Information Risk Owner (SIRO): The Force SIRO is the Deputy Chief Constable. The SIRO is responsible for the setting the information risk appetite and risk tolerance parameters.

Information Asset Owner(s) (IAO's): IAO's are senior/responsible individuals within the Force who are the nominated owners of one or more identified assets, including cloud hosted solutions. They are required to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information and ensure that information is fully used within the law for public good, and provide assurance to the SIRO that the appropriate security measures are in place to protect their assets. Information Asset owners are responsible for ensuring that assets are used appropriately for the storage and retention of records. They are responsible for ensuring that review &/or automated deletion timescales are set in accordance with NPCC Records Retention Guidance.

Records Management Unit: Records Management Unit staff are responsible for making decisions in respect to the matching and retention of records. They will also provide support to the Records and Data Quality Supervisor by responding to records management enquiries, providing advice and guidance and escalating to the Records and Data Quality Supervisor where appropriate.

Data Protection Officer: The Data Protection Officer performs the protected statutory and independent role of Force Data Protection Officer and is the responsible officer for the provision of strategic advice, planning, and compliance with all aspects of the Data Protection Act 2018, UK,General Data Protection Regulation and associated legislation and guidance.

Officers, Staff and Volunteers: Officers, staff and volunteers will ensure that all information created, received and held, for which they are responsible is secure, accurate, relevant, kept up to date and retained or disposed of in line with Force policies/procedures and the Retention Schedule.

Business area leads/departmental managers have ownership of records within their business area. All business area leads / managers will:

- Ensure that all information and assets created, received and held, for which they are responsible, is secure, accurate, relevant, kept up to date and reviewed/retained or
- Disposed of in line with the Force Retention and Destruction Schedule
- Ensure that all officers, staff and volunteers are involved in the implementation of records management through internal communication, profile raising, publicity and training
- Ensure that appropriate resources are available to properly maintain their business area's records
- Publish accurate procedural guidance, support and tools designed to help each person in that business area manage and use the information effectively and in accordance with the APP on information management, relevant policies and supporting guidance.
- Where local procedures dictate a deviation from the APP on information management, the full rationale will be documented and authorised.
- Conduct and record periodic data quality assurance audits on the information held in their business area to ensure that Data Quality Standards and recording principles are complied with and utilise performance information to provide feedback and support where appropriate.
- Conduct and record annual audits of the information held in their business area to ensure the ongoing compliance with the Force Records Management Policy, the Force Records Retention Schedule and other appropriate local and national policies and procedures.
- Ensure that the records in their business area are backed up, that disaster recovery processes are in place to ensure business continuity and that the records can be preserved over time.

Line Managers: Shall be responsible for ensuring security processes are followed to protect the physical environment where information is processed or stored. They are also responsible for ensuring that officers, staff and volunteers are aware of the information security policies and procedures applicable in their work areas, their personal responsibilities for information security, and how to access advice on information security matters. It is also the line manager's responsibility to make sure officers, staff and volunteers know how to report a security breach.

Code of Ethics

The nine Policing Principles of the Code of Ethics:-

- Accountability - You are answerable for your decisions, actions and omissions. (Through data quality audits and records management, officers, staff and volunteers will be held accountable for the quality of records created)
- Fairness - You treat people fairly. (Consistency will be applied when reviewing records for deletion/ retention)
- Honesty - You are truthful and trustworthy.
- Integrity - You always do the right thing. (Records will be created and managed strictly in accordance with approved practice)
- 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

These principles underpin and strengthen the existing procedures and regulations for ensuring standards of professional behaviour for police officers, staff and volunteers.

All 9 principles are relevant to this policy.

5. Take action and review

The **SIRO** and **Information Assurance Board** will be kept informed of the records management status of the Force by means of regular reports and meetings. The Information Assurance Board meets on a quarterly basis. The Data Protection Officer reports regularly to the SIRO.

Records management processes will be subject to regular audit to ensure their effectiveness in delivering records management services which adhere to requirements of law and comply with best practice promoted via MoPI guidance. These processes and this policy shall be subject to audit by the Force's internal and/or external auditors as necessary. Findings will be reported to the SIRO and the Information Assurance Board.

The Records and Data Quality Supervisor who has the responsibility for this policy, will update the policy in line with relative changes in legislation, ICO guidance, College of Policing guidance, NPCC guidance etc.

Compliance with this policy will be monitored via:

- Data Protection and Information Security breach reporting processes
- Internal information Data Protection Compliance Audits
- Independent audit.

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.

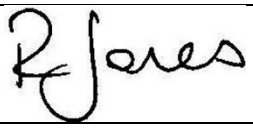
Carrying out an **equality impact assessment** involves systematically assessing the likely or actual effects of policies on people in respect of all the protected characteristics set out above.

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.

Equality Impact Assessment Completed	
Name:	Records & Data Quality Supervisor
Department:	Records Management Unit, IMBA
Signed:	M. James
Date:	2nd November 2023

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:	Head of Legal Services
Department:	Legal Services
Signed:	
Date:	17 October 2023

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:	Records & Data Quality Supervisor
Department:	Records Management Unit, IMBA
Signed:	M. James
Date:	17/10/23

CORPORATE FINANCE REVIEW

No changes to this policy will incur any financial cost other than to amend, improve or formalise business as usual practices that are affordable and within budget. Any policy change affecting financial cost must be discussed with the Corporate Finance department in advance of seeking approval of this policy. Please sign to confirm that the financial impact of this policy area has been considered and that Corporate Finance have been notified of any change, if applicable.

Name:	Head of Corporate Finance
Department:	Corporate Finance
Signed:	
Date:	07/12/2023

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	17/10/23	M. James
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.			
Harm – in publication			None

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.			

Full Version Control

Version	Date	Author	Rationale
1	21/12/2011		First Version
2	06/11/2012		Rewrite policy to reflect launch of Authorised Professional Practice (Decision Making)
3	16/07/2013		Revision to reflect change in departmental structure
4	19/05/2015	Information Manager	Review and update to reflect changes following Public First departmental changes
5	21/02/2018	Information Manager	Annual review – change of policy template to reflect Code of Ethics. Policy updated as a result
6	04/02/2021	Records & Data Quality Supervisor	To reflect changes to APP MoPI Guidance
7	17/10/2023	Records & Data Quality Supervisor	Policy Review

Heddlu Police
DYFED-POWYS