WILTSHIRE POLICE & POLICE AND CRIME COMMISSIONER

INFORMATION MANAGEMENT POLICY

Date of Publication: February 2021
Version: 3.0
Next Review Date: February 2023

TABLE OF CONTENTS

POLICY STATEMENT

Information is the lifeblood of policing. It underpins our operational activities, processes and systems leading to effective investigations, timely arrests and improved criminal justice outcomes. It also helps to prevent further crimes being committed and is vital in the fight against crime.

Information Management describes the means by which an organisation efficiently plans, collects, organises, uses, controls, shares, disseminates and disposes of its information, and through which it ensures that the value of that information is identified and exploited to the fullest extent.

Rationale

Wiltshire Police and the Office of the Police and Crime Commissioner (OPCC) have a duty to obtain, use and lawfully share a wide variety of information with our partners in order to discharge our collective duties effectively and keep communities safe. The collection, exploitation and sharing of information is an essential function of policing. Managing information effectively is crucial for:

- keeping people safe
- providing evidence to investigate, prosecute and prevent crime
- managing the business
- mitigating risks around the poor use of information such as non-compliance with legislation, harm to the public and loss of reputation.

The Information Management policy and any supporting System Operating Procedures (SOPs) and guidance are required to reflect legal obligations and national policy. These include but not necessarily limited to:

- The Code of Practice on the Management of Police Information (MoPI) and the Authorised Professional Practice (APP) for Information Management
- UK-GDPR
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990

It will ensure that all staff, including our partners, understand their responsibilities with information and are provided with the knowledge and standards to use that knowledge in line with legislative requirements and in pursuance of our policing vision and aims.

Intention

The Information Management policy in conjunction with supporting SOPs and guidance, sets out how Wiltshire Police will ensure that information is managed effectively and lawfully throughout its lifecycle.

This policy is intended to provide officers, police and OPCC staff, contractors, volunteers and other relevant parties with clear and concise guidance that enables them to create, use, retain and dispose of information appropriately, lawfully and with confidence.

The policy is intended to enable consistent and transferable procedures and information sharing across other police, government and partnership organisations.

The Chief Constable has a responsibility under the Management of Police Information (MOPI) Code of Practice to establish and maintain an Information Management Strategy (IMS) under the direction of a Chief Police Officer or equivalent. This policy and supporting SOPs and guidance cover the key points of an IMS as defined by the Authorised Professional Practice (APP) on Information Management and is therefore intended to fulfil that requirement.

1. APPLICABILITY

This policy applies to everyone with access to the OPCC and Forces' information, whether employees, contractors, volunteers, professional partners and employees of other organisations, and whether on police or partner premises, or working remotely.

The policy applies to all information, whether held digitally or in paper or other physical format. This includes (but is not limited to) text, data, images, and voice and video recordings, and covers both structured material (e.g. Force IT systems and databases) and unstructured material (e.g. documents, emails).

Records are documents or data that provide evidence of the Forces' actions and decisions and are required for legislative and audit purposes, as well as providing an 'organisational memory'. Generally the same principles contained within this policy should be taken as applying to both information and records.

The policy applies to both personal[1] and non-personal information and covers all information gathered for the effective running of the organisation. This includes information required for 'Law enforcement purposes', which is defined by the Data Protection Act 2018 as necessary for the:

- prevention, investigation, detection or prosecution of criminal offences, or
- execution of criminal penalties, including the safeguarding against and
- prevention of threats to public security.

The Law enforcement purposes provide the legal basis for the collecting, recording, evaluating, sharing and retaining of police information.

Information held for Law enforcement purposes specifically includes (but is not limited to) the following business areas:

- Crime Management
- Intelligence
- Public protection
- Custody

2. PRINCIPLES

The key information management principles are as follows:

Responsibility

Information management is everyone's responsibility and they must ensure that information is used appropriately and in accordance with the force Values and Behaviours, Code of Ethics and Data Protection Act 2018 (includes: General Data Protection Regulations (UK-GDPR)).

Accessibility and Re-use

All information obtained or created for organisational or policing purposes belongs to Wiltshire Police and/or the OPCC. It must be treated as an organisational asset, and managed and stored in an authorised system and/or location.

Wherever feasible, information should be recorded only once and all policing information concerning an individual (also referred to as 'a nominal') should be linked so that it is easily retrievable.

[1] As defined by the Data Protection Act 2018

All information should be in a form which facilitates re-use and interoperability across the Force, and with other Forces where appropriate.

Wherever feasible, information should be migrated to newer formats and / or systems when the current ones become obsolete.

Quality

All information should be accurate, adequate, relevant and timely, and recorded in a manner appropriate for potential future disclosure, and in accordance with national and legal requirements.

In regard to information held for a policing purpose, the information should comply with the principles of the National Intelligence Model (NIM), and should be evaluated, graded and recorded accordingly. Where appropriate, the source of the information, the nature of the source, any assessment of the reliability of the source, and any necessary restrictions on the use to be made of the information will be recorded to facilitate later review, reassessment and audit.

Data quality audits and data improvement initiatives will be carried out where appropriate.

Quantity

The quantity of any information, especially personal information, which is captured and retained should be proportionate to the Law Enforcement Purpose or business requirement.

Security

Safeguards to the information held by the force are documented in the Information Risk Management Policy and achieved through compliance with this policy, other policies, standards and guidance.

Appropriate safeguards must be put in place to protect personal, sensitive and/or information classified under the Government Security Classification Scheme (GSC) (see Government Security Classification Guidance Handout for details). The extent of the safeguards should be in proportion to the degree of risk posed.

The Government Classification Scheme (GCS) details how information should be marked and handled. All information sent via email or post must be dispatched in accordance with the requirements stated on page 2 of the Government Security Classification Guidance Handout.

Disclosure

The ethos of MoPI is that information should be re-used in order to fulfil a Law Enforcement Purpose and/or to protect the public from harm. However, the Force is also required to comply with the law and therefore information may only be accessed, shared or disclosed internally or externally when it is considered appropriate to do so.

Particular care should be taken with personal, sensitive and/or information classified under the GSC to ensure sharing is lawful and proportionate. Information Sharing Agreements (ISAs) should be put in place where personal data is being regularly disclosed to or received from partners, and Data Processing Agreements (DPAs) drawn up where one party is processing information on another party's behalf.

Any ISAs or DPAs should be written in accordance with the good practice advice and guidance provided by the Data Protection Officer (DPO) and Force Solicitor. A library of current ISAs and DPAs will be maintained by the DPO.

Transparency

It is the Forces' and Police and Crime Commissioner's policy to fully comply with the Freedom of Information Act 2000. Information which is not exempt from disclosure will be made available on request.

Retention

All information, particularly personal data, should not be retained longer than necessary. Information obtained for Law Enforcement Purposes will be reviewed, retained and disposed of on a risk assessment basis, and in accordance with the APP on Information Management, wherever practical. In all other cases, time-based disposals will be applied, in accordance with Force Records Retention Schedule and the National Police Chiefs' Council Retention Schedules where applicable.

Risk Management

Information management risks will be considered, and appropriate mitigations implemented, whenever significant changes are made to Force processes or systems. Where personal data is being processed, this will require the completion of a Data Protection Impact Assessment (DPIA).

3. ROLES AND RESPONSIBILITIES

Overall responsibility for Information Management rests with the Chief Constable as **Data Controller** for the Force and the Police and Crime Commissioner for the OPCC.

The Senior Information Risk Owner **(SIRO)** holds responsibility for overseeing all central functions for Information Management and for making strategic decisions in regard to information risks across Wiltshire Police and OPCC, particularly when there is a potential conflict between operational and security requirements.

The term Information Asset Owner **(IAO)** is used for the corresponding function at project, programme or organisational unit level.

Where appropriate, senior business leaders will be appointed as IAOs to provide governance and oversight for significant information assets. They are responsible for ensuring this information is managed in accordance with this policy and are accountable for the confidentiality, integrity and availability of their information asset.

The Information Governance Strategy Board (**IGSB**) is the governance authority that commissions and approves all activities, policies, standards and guidelines in support of the Wiltshire Police/OPCC Information Strategy.

The **Head of Information Management & Assurance / DSIRO** has responsibility for maintaining all information policies and ensuring that risks to the Forces' information are appropriately managed.

The Data Protection Officer (DPO) responsibilities include; monitoring internal compliance with DP legislation, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs), acting as a contact point for data subjects and the Information Commissioner's Office (ICO).

The **Force Records Manager** and the **Force Operations Manager, Justice** are responsible for the provision of advice in relation to records management and leadership in the maintenance and development of records management facilities, standards and practices in order to secure the Force's compliance with records management legislation and guidance.

The **Force Disclosure Unit** provides services and advice in relation to information sharing and disclosure under the Data Protection and the Freedom of Information Acts.

All **Managers and supervisors** have responsibility to ensure their staff is aware of, and adhere to, policies and procedures relating to information management and the appropriate use of information systems. They are also responsible for identifying any local risks relating to information and escalating them if appropriate, in accordance with the Information Risk Management Policy.

Expectation of all staff

All those who access and use Force information are responsible and accountable for the information they handle whether on computers, on paper, or through the spoken word. Training determined through agreement with Learning and Development and IAOs must be completed and all must be familiar with the requirements of this policy, and relevant procedures and standards.

Supporting SOPs and Guidance

While the intention of this Information Management Policy is to provide clear and concise direction, considerably more detail is necessary to provide clear procedural requirements and guidance. Such detail will be contained in a set of SOPs and guidance, produced by Business Area leads/Managers, which are to be regarded as policy in so far as compliance with their instruction is required.

Further advice and guidance can be obtained from the Force Policy and Procedures site.

Implementation Strategy

This policy will be available via the intranet and on the public website. It will also be circulated for the attention of staff.

POLICY AIM

The aim of this policy is to ensure that all Force and OPCC information is held lawfully and is readily accessible on demand; promote consistent management of all records throughout their lifecycle; ensure all information is captured and maintained in such a way that its evidential weight and integrity is not compromised; promote auditable decision-making and to maintain information management best practice.

LEGAL BASIS AND DRIVING FORCE

This policy is underpinned by:

- the Data Protection Act 2018,
- UK GDPR
- the Human Rights Act 1998,
- Freedom of Information Act 2000,
- Computer Misuse Act 1990, and
- College of Policing (COP) Authorised Professional Practice (APP) on Information Management.

RELATED POLICIES, PROCEDURES and OTHER DOCUMENTS

Records Management Policy
Information Security Policy

System Operating Procedures (SOPs)
Freedom of Information Policy
Data Protection Policy
Force Records Retention Schedule
National Police Chiefs' Council Retention Schedules
Home Office Code of Practice on the Management of Police Information (MoPI)
Government Security Classification Guidance Handout

AUTHORISED PROFESSIONAL PRACTICE

Information management
National Intelligence Model (NIM)

DATA PROTECTION

Any information relating to an identified or identifiable living individual recorded as a consequence of this policy will be processed in accordance with the Data Protection Act 2018, General Data Protection Regulations and the Force Data Protection Policy.

FREEDOM OF INFORMATION ACT 2000

This document has been assessed as suitable for public release.

MONITORING AND REVIEW

This policy will be reviewed every two years by the Force Records Manager, or in response to significant changes in Force strategy, national policy or legislation.

WHO TO CONTACT ABOUT THIS POLICY

The Information Management and Assurance Business Area is responsible for this policy. All queries relating to this policy should be directed to the Records Manager or Force Policy Officer.

DOCUMENT ADMINISTRATION

Ownership:

Department Responsible: Information Management and Assurance
Policy Owner/Author: Keith LEWIS / Leonie CALLAND
Technical Author:
Senior Officer/Manager Sponsor: Deputy Chief Constable

Revision History:

Revision Date	Version	Summary of Changes
10.11.2020	2.0	Reference and link to the Government Security Classification Guidance Handout added.
08.02.2021	3.0	Procedure amended to include reference to the OPCC.

Approvals:

This document requires the following approvals:

Name & Title	Date of Approval	Version
Force Policy Officer		
SLT – Keith LEWIS		
JNCC (Not required for all policies)	N/A	

Distribution:

This document has been distributed via:

Name & Title	Date of Issue	Version
E-Brief		
Email to relevant affected Staff/Officers		
Other: (state method here)		

Diversity Impact Assessment:

Has a DIA been completed? If no, please indicate the date by which it will be completed. If yes, please send a copy of the DIA with the policy.	☒ **Yes** ☐ **No** **Date**:

Consultation:

List below who you have consulted with on this policy (incl. committees, groups, etc):

Name & Title	Date Consulted	Version

Implications of the Policy:

Training Requirements

None.

IT Infrastructure

None.