Policy Title: **Information Management**

Date Published/Reviewed: **September 2021**

Thames Valley Police and the Hampshire Constabulary ensure that all policies have been assessed and comply with MoPI Guidance, and the Data Protection Act 2018. In addition, this Policy has been reviewed by each Force's Head of Health, Safety and Environment and has undergone an Equality Impact Assessment.

1.0 About this Policy

1.1 Rationale

1.1.1 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 organisation and enabling effective decision making, transparency and accountability
- handling personal data appropriately
- mitigating risks around the poor use of information such as non-compliance with legislation, harm to the public and loss of reputation
- working effectively with partners
- enabling citizens to exercise their rights in regard to their personal data.

1.2 Legislation/National Standards

1.2.1 The Information Management policy and any supporting guidance are required to reflect legal obligations and national policy. These include:

- the Code of Practice on the Management of Police Information (MoPI) and the Authorised Professional Practice (APP) for Information Management
- Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Official Secrets Acts 1989
- Computer Misuse Act 1990.

1.3 Intention

1.3.1 The Information Management policy and supporting guidance set out what Hampshire Constabulary and Thames Valley Police shall do and how they shall ensure that information is managed effectively and responsibly as a valuable corporate asset throughout its lifecycle, so that it is accurate, relevant and accessible whenever it is needed.

1.3.2 The policy is intended to provide clear and concise direction that enables all individuals with access to the Forces' data to create, access, use, retain and dispose of information appropriately, lawfully and with confidence and to ensure the appropriate handling of personal data to protect data subjects' privacy rights and in accordance with the UK GDPR and the DPA 2018.

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

1.3.4 MoPI requires each Force to have a current 'Information Management Strategy' (IMS). This policy covers the key points of an IMS as defined by the APP on Information Management and is therefore intended to fulfil that requirement.

1.4 Scope

1.4.1 This policy applies to both Hampshire Constabulary and Thames Valley Police, and shall operate in accordance with the collaboration arrangements for Information Management.

1.4.2 The policy applies to everyone with access to Force data and information, whether employees, contractors, volunteers, professional partners and employees of other organisations, and whether on police or partner premises, or working remotely.

1.4.3 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. emails, documents, social media content).

1.4.4 The policy applies to both personal[1] and non-personal information.

1.4.5 The policy covers all information gathered for the effective running of the two Forces, i.e. operational and non-operational.

1.4.6 Some information is defined by MoPI as being necessary for a 'policing purpose':

- 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.

1.4.7 Information held for a policing purpose specifically includes (but is not limited to) the following business areas:

- Crime data collection and recording
- Contact management
- Crime management
- Intelligence
- Public protection
- Firearms licensing
- Custody.

1.4.8 In regard to information held for a policing purpose, this policy applies to all information collected or recorded from April 2006 onwards[2]. Older material will be brought into scope wherever it is feasible and cost-effective to do so.

1.4.9 Records are documents, information or data that provide evidence of the two Forces' actions and decisions and are required to be kept 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. Specific management processes for records will be defined by the Joint Information Management Unit (JIMU) where appropriate.

[1] As defined by the UK GDPR and the DPA 2018

[2] The date the Code of Practice on the Management of Police Information came into effect

2.0 Statement of Policy

2.1 The Information Management Policy covers ten key areas:

1. Responsibility	Information management is everyone's responsibility and everyone must ensure that information is stored, managed and used appropriately, and in accordance with this policy and the Code of Ethics.
	Anyone who has access to Force information must complete mandatory induction, training and refresher training relating to information management, data protection and security. Additional training may be specified dependent on role.
	Specific roles and responsibilities for information management are set out in the guidance which accompanies this policy.
2. Accessibility and reuse	Information obtained or created for organisational or policing purposes belongs to the relevant Force. It must be treated as an organisational asset, and managed and stored in an authorised system and/or location.
	Information must only be accessed and used when it is appropriate and necessary to do so. The Forces will use all appropriate mechanisms to control and audit access.
	Wherever feasible, information should be recorded only once and policing information concerning an individual (also referred to as 'a nominal') should be linked so that it is easily retrievable.
	Information should be in a form which facilitates reuse and interoperability across each Force, and with other Forces where appropriate and where there is a legal basis for sharing.
	Wherever feasible, information should be migrated to newer formats and / or systems when the current ones become obsolete. In particular, personal data should be kept in a format that enables 'right to erasure' and 'right to rectification' to be exercised efficiently.
3. Quality	Information shall be accurate, adequate, relevant and timely. It should be recorded in accordance with national and legal requirements, and in a professional manner appropriate for potential future disclosure.
	In regard to information held for a policing purpose, 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. It should be also possible to distinguish clearly between fact and opinion.
	Data quality audits and data improvement initiatives shall be carried out where appropriate.

4. Quantity	The quantity of any information captured and retained should be proportionate to the policing purpose or business requirement. Personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')" in accordance with UK GDPR Article 5(1)(c).
	Personal data retained beyond its original purpose for research or statistical use should be anonymised or pseudonymised wherever feasible.
5. Security	Information shall be stored, managed and handled in accordance with the Forces' Information Security Policy, standards and processes.
	All newly created information is classified as OFFICIAL or above, dependent on the sensitivity, under the Government Classification Scheme (GCS)[3]. Any material classified under the GCS or the earlier Government Protective Marking Scheme (GPMS) must be managed appropriately, following the relevant guidance and handling instructions.
	The extent of the safeguards taken to protect information should be in proportion to the degree of risk posed to individuals and/or operations and/or the organisation. Particular care must be taken with personal data, sensitive and/or classified information.
	All security incidents, including lost, compromised or inappropriately disclosed information or personal data, must be reported immediately using the online reporting tool. Any potential Data Protection breaches will be assessed by JIMU and reported to the Information Commissioner's Office if appropriate.
6. Appropriate disclosure	MoPI encourages the reuse and linking of information in order to fulfil a policing purpose and/or to protect the public from harm. However, the two Forces are also required to comply with the law and therefore information may only be shared or disclosed internally or externally when it is considered appropriate and proportionate to do so.
	Particular care shall be taken when sharing personal, sensitive and/or information classified under the GPMS / GCS. Information Sharing Agreements (ISAs) must be put in place where personal data is being regularly disclosed to or received from partners, and Data Processing Agreements (DPAs) drawn up where a third party is processing information on behalf of either or both Forces.
	In order to comply with the UK GDPR and the DPA 2018, any ISAs or DPAs should be written in accordance with APP and with advice from JIMU. A library of current ISAs is available on the Forces' intranets and websites.

[3] The GCS was adopted by Hampshire Constabulary and Thames Valley Police on 1 October 2016.

7. Data subjects' rights	The two Forces will respond appropriately to requests from individuals (data subjects) to exercise their rights concerning their personal data, in compliance with the UK GDPR and DPA 2018.
	The legislation usually requires the organisation to respond within one month and therefore any request concerning an individual's personal data must be passed to JIMU immediately for efficient processing.
8. Transparency	Information which is not exempt from disclosure under the Freedom of Information Act shall be made available on request, and information of public interest will be proactively published on the Force websites wherever feasible.
	Data privacy notices shall be published and regularly reviewed in accordance with UK GDPR and DPA 2018 requirements, including information to describe what personal data is collected, how it is processed and how data subjects may request to exercise their rights.
	An 'Appropriate Processing Document' (APD) shall be published and regularly reviewed alongside the data privacy notice that sets out how Hampshire Constabulary and Thames Valley Police will protect special category and criminal conviction personal data in compliance with UK GDPR and the DPA 2018.
9. Retention	Information, particularly personal data, should not be retained longer than necessary.
	Individuals must ensure that data, information or paper files that need to be retained as an organisational record are stored appropriately in accordance with Force guidance and advice from JIMU.
	Information obtained for a policing purpose shall be reviewed, retained and disposed of on a risk assessed basis, and where feasible, in accordance with the APP on Information Management.
	In all other cases, time-based disposals shall be applied, in accordance with the National Police Chiefs' Council Retention Schedules and any local retention policy.
	Where routine review and disposal is not feasible or cost-effective, safeguards shall be put in place to minimise any potential detriment caused by continued retention of personal data. In addition, JIMU shall review material by exception, should individuals exercise their rights in regards to requesting rectification and/or erasure of their personal data.
	The APD shall retained for six months beyond the cessation of processing of all sensitive personal data. (However it is envisaged that Hampshire Constabulary and Thames Valley Police will always be processing such data due to the nature of their public function.)

10. Risk management and Data Protection Impact Assessments	Information management risks shall be considered, and appropriate mitigations implemented, whenever significant changes are made to Force processes or systems. Where personal data is being processed, this will usually require the completion of a Data Protection Impact Assessment (DPIA), under the guidance of JIMU.
	JIMU shall lead a regular information risk review process with Information Asset Owners and Data Guardians. Significant risks shall be captured on risk registers and escalated to the Joint Information Management Board if appropriate.

2.2 Monitoring

Compliance with this policy shall be monitored by a number of methods under the advice and/or direction of the Data Protection Officer, including:

- Information Asset risk assessments
- Analysis of reported data incidents
- Targeted and ad hoc monitoring of information systems usage
- Identification of trends and escalation of concerns to the Joint Information Management Board
- Independent audits.

3.0 Human Rights Articles Engaged

Article 8: Right to a private and family life.

4.0 Health and Safety at Work

No Health & Safety implications have been identified.

5.0 Communications, Challenges and Representations

5.1 Communication

This policy shall be made available in the Policies & Procedures intranet section and the Forces' public websites.

5.2 Challenges and representation

Head of Information Management
Joint Information Management Unit
Thames Valley Police HQ
Oxford Road
Kidlington

Oxfordshire
OX5 2NX

6.0 Review Date

This policy shall next be September 2023

7.0 Related Guidance

Information Management APP

8.0 Freedom of information

Suitable for publication.

9.0 Government Security Classification Policy

This policy document shall be marked as Official.