Wiltshire Police

Records Management Policy

Document History

Version Number	Date of Issue	Author	Reason for Issue
Draft v0.1	March 2007	Martin Root	Initial Draft
Draft v0.2	August 2007	Martin Root	Revised Draft
Draft v0.3	May 2008	Simon James	Revised and updated
Version 0.4	26 January 2009	Michael Ngero	Updated
Version 0.5	17 February 2014	Michael Ngero	Reviewed and updated
	February 2016		**Next Review Date.**

INTRODUCTION

Statement of Policy

Wiltshire Police recognises that the efficient management of its records is necessary to comply with its legal and statutory obligations including the Management of Police Information Code of Practice, Guidance and other codes of practice. Dynamic records management will contribute positively to the performance, efficiency, continuity and productivity of the force strategic policing aims and objectives.

Records owned and managed by Wiltshire Police are its organisational memory, providing evidence of actions and decisions, and represent a vital asset to support the Force's daily functions and operations. The Force will record and maintain records that are complete, authentic, reliable, secure and accessible, and manage those records in accordance with good practice, including legislative requirements throughout their lifecycle.

Aim of Policy

To competently record and manage all information held for policing activity in an efficient and consistent manner to support the objectives and vision of Wiltshire Police and ensure that national and local objectives are met.

Glossary of Terms

Term	Meaning
ACPO	Association of Chief Police Officers
CoP	Code of Practice
FISP	Force Information Security Policy
MoPI	Management of Police Information
ISCSP	Information Security Community Security Policy
PSFP	Police Service File Plan
QA	Quality Assurance
Syops	Systems Operating Protocols

Strategic Aims

To:

- ensure that within all Force 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;
- maintain good practice information management;
- reduce costs of records storage and management, including retrieval and controlled disposal.

RECORDS MANAGEMENT WITHIN WILTSHIRE POLICE

Information, knowledge and intelligence are the lifeblood of policing. Once captured, they must be systematically managed as business records according to the records management policy and standard working principles highlighted within this document.

Scope

A record is defined as "information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business." (BS ISO 15489: 2001).

This policy, together with the associated standards, applies to the management of all records in all technical or physical formats or media, created or received by staff of the Force in the course of carrying out the functions of the organisation.

Although not an exhaustive list, examples of items that can constitute records include: -

- Documents (including written and typed documents and annotated copies)
- Computer files (including word processor files, databases, spreadsheets and presentations)
- Electronic mail messages
- Diary records
- Fax messages
- Brochures and reports
- Intranet and Internet Web pages
- Forms
- Seized evidence
- Audio and video tapes, including CCTV
- Microfiche and microfilm
- Maps and plans
- Photographs

Benefits of Records Management

Records management supports the business enterprise by ensuring that information is managed throughout its life cycle in a systematic, cost-effective and efficient manner. Adherence to efficient records management practices will enable Wiltshire Police to meet its statutory objectives and business responsibilities as a dynamic organisation. Knowledge and information must remain protected, accurate, ordered, complete, useful, up to date and accessible whenever it is needed to:

- Drive our Policing Plan and wider policing vision.
- Facilitate informed decision making at all levels and locations.

- Protect the rights of employees, stakeholders, clients, legal entities and the general public.
- Promote the activities and achievements of the organisation.
- Ensure that Wiltshire Police operates effectively as a prosecuting authority and meets its lawful obligations with regards to the disclosure of evidence.
- Reduces the cost in finding and managing information
- Promotes best value in terms of human and space resources.
- Support innovative research and development.
- Ensure compliance with relevant legislation
- Ensure that precedents are identified accurately.
- Support continuity and consistency in management and administration.
- Provide an audit trail to meet business, regulatory and legal requirements.
- Provide an historical perspective.

Relationship with existing legislation, standards and policies

This document has been drawn up within the context of:

- Management of Police Information (MoPI) Code of Practice (CoP) and Guidance
- Force Information Management Strategy (FIMS)
- Review, Retention and Disposal policy (RRD)
- Force Information Sharing, Disclosure and Dissemination policies
- ISO 15489-1:2001 (Information and documentation -- Records management -- Part 1)
- ISO 17799:2005 (Information technology - Security techniques - Code of practice for information security management)
- BSI BIP 0025-1:2002 (Effective records management. A management guide to the value of BS ISO 15489-1)
- BSI BIP 0025-2:2002 (Effective records management. Practical implementation of BS ISO 15489-1)
- BSI BIP 0008:2004 (Code of practice for legal admissibility and evidential weight of information stored electronically)
- BSI BIP 0009:2004 (Legal admissibility and evidential weight of information stored electronically. Compliance workbook)
- BSI BIP 0010:2004 (The principles of good practice for information management)
- Force Information Security Policy (FISP),
- ACPO/ACPOS Information Security Community Security Policy (ISCSP),
- Quality Assurance and Audit (QA),
- Force Systems Operating Protocols (SyOPs)

STANDARD WORKING PRINCIPLES

General Principles

Central to the implementation of systematic records management within an organisation is the development of a business classification scheme or file plan.

To ensure that Force records are complete, reliable, authentic, secure and accessible, the following will be adhered to:

- records will be stored so as to provide adequate protection against unauthorised access or damage;
- records will be readily available to meet operational need and legal obligations;
- records will be disposed of promptly in accordance with the Retention (Disposal) Schedule and an audit trail kept;
- records management systems will provide an auditable trail of records transactions from creation through to ultimate disposal;
- divisional/departmental compliance with this policy will be reviewed as part of Performance Management.

Records management good practice recognises that a record can be in any format and has a defined lifecycle. A record also requires metadata to ensure that it is managed systematically. Metadata should be based upon a business classification scheme (or file plan) and should stay with the record until the point of disposal when the record is no longer needed for business purposes. This is governed by a retention (or disposal) schedule that sets out the period for retaining a given record type. During or at the end of the retention period the record is reviewed and a disposal decision is made, which might be to retain the record for a further period of time, pass the record to another organisation or to destroy the record.

2. Functions and Responsibilities

The Force has a corporate responsibility to maintain its records and record keeping systems in accordance with good business practice and its legal obligations. The person with overall responsibility for this policy is the Chief Constable.

2.1 ACPO

Chief Officers have overall responsibility for Wiltshire Police records management policy and standard working principles, and for supporting the application of the policy and principles Force-wide.

ACPO staff will:

- ensure clear lines of accountability for records management;
- monitor and review systems in place for records management at least annually in order to make improvements;
- seek independent assurance that an appropriate and effective system of managing records is in place.

2.2 Records Manager

The Records Manager will have the following responsibilities:

- To develop, implement and maintain the records management standard working practices that underpins the records management policy.
- to provide a single point of contact to system and process owners;
- to ensure review, retention and disposal schedules are implemented;
- to ensure that the records management policy and principles are kept up-to-date and relevant to the needs and obligations of the Force through consultation and assessment against external standards;
- to determine records management relationships with internal and external stakeholders, including audit and management teams;
- to monitor individual and Force compliance with the records management policy and principles.
- to manage the storage conditions of all records on-site and off-site including contract storage services;

2.3 Senior Management (Business Process and System Owners)

Ownership of the business record lies with the head of each business area. Where there is no clearly defined business owner of a record, then ownership for disposal purposes will default to the Records Manager.

Senior Managers will:

- collaborate with the Records Manager to define the service levels where policy and principles are not explicit;
- take active responsibility for records management and for ensuring that all staff are involved in the implementation of the records management strategy, through internal communication, profile raising, publicity and by ensuring appropriate resources and training.

2.4 All Staff

All staff within the Force will ensure that all records and information created, received and held, for which they are responsible, is accurate, relevant, kept up to date and disposed of in accordance with the Force's records management policy and standard working principles. This responsibility is established at, and defined by, law; and is included in terms of employment.

All staff have a responsibility to implement Wiltshire Police records management policy and standard working principles;

3. Records Management System

The Force will develop a co-ordinated records management system to ensure that the characteristics of records are maintained throughout their lifecycle and that records are credible and authoritative.

Authenticity

It must be possible to prove that records are what they purport to be, that their integrity is demonstrably intact, and it must be possible to identify who created them. Where information is added, an audit trail of the added information will be created.

Accuracy

Records will accurately reflect the transactions that they represent.

Integrity
Records will be securely maintained to prevent unauthorised access, alteration, damage or removal. They will be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents. Where records are migrated across changes in technology, the Force will ensure that the evidence preserved remains authentic and accurate.

Usability
Records will be readily available and sufficient in content, context and structure to provide sufficient authenticated evidence of the relevant activities and transactions. This includes the accessibility and use of electronic records for as long as required (which may include their migration across systems); and the ability to cross reference electronic records to their paper counterparts in a mixed environment.

3.2 **Record capture**

The purpose of capturing items as records is to: -

- establish a relationship between the record, the creator and the business context that originated it,
- place the record and its relationship within a records system,
- link it to other records, and
- ensure that appropriate audit trails are maintained

Clearly worded and effectively disseminated procedures, rules and conventions relating to each police system/process will be essential to the success of recording information accurately and then filing them in a dynamic environment. Records should indicate:

- what types of information should be submitted to and recorded upon specific systems;
- the necessary fields required for a complete person record, meeting the minimum requirements of forename, family name, partial name, nickname or alias;
- the details that need to be included when submitting and recording information;
- the conventions for recording information;
- acceptable timescales for submitting and recording information;
- rules for linking information within and between systems;
- full explanations for the use of any categorisation/codification schemes associated with systems or types of information.

Each operational/business area will have in place an adequate system for documenting its activities and processes. This system will take into account the legislative and regulatory environments in which the operational/business area works.

3.3 Registration

The primary purpose of registration is to provide evidence that a record has been created or captured in a records system and an additional benefit is that it facilitates retrieval. It involves recording brief descriptive information or metadata about the record and assigning the record a unique identifier. Registration formalises the capture of the record into the records system.

In a records system which employs registration processes: -

- a record is registered when it is captured into the records system (this may include the placing of a manual record into a structured filing system or the automated registration of electronic records in an electronic record keeping system); and
- no further processes affecting the record can take place until its registration is complete.

Records may be registered at more than one level or aggregation within a records system. In the electronic environment, records systems may be designed to register records through automatic processes, transparent to the user of the business system from which it is captured and without the intervention of a record manager.

3.4 Classification

Classifying information is a vital discipline. Good practice dictates a functional rather than an organisational structural approach. At the top level the classes cover the key functions for which the organisation is responsible. Below that are the activities that define each function and the transactions or processes that comprise them.

The Force will have in place a record classification system (the PSFP, or similar) based on the business activities which generate records, whereby they are categorised in systematic and consistent way to facilitate:

- ensuring records are named in a consistent manner over time;
- linkage between individual records that accrue to provide a continuous record of activity;
- retrieval of all records relating to a particular function or activity;
- assessment of security protection and appropriate access for sets of records;
- distribution of responsibility for management of particular sets of records;
- evaluation of appropriate retention periods and disposition actions for records.

3.5 Indexing

Indexing can be done manually or automatically generated. The function of an index or referencing system is to provide the user with an efficient means of tracing and finding information.

The Force will implement an indexing/referencing system that enables the user to:

- immediately establish the presence or absence of information on a given subject;
- identify and locate relevant information within a set of records;
- group together information on subjects.

3.6 Metadata

As well as the content, the record will contain, be linked to, or associated with, metadata which is descriptive and technical documentation about the file or document such as:

- how, when, and by whom it was received, created, accessed, and/or modified and how it is formatted;
- when the disposal of electronic records should occur, for this must be included in the metadata when the record is created.

3.7 Records Maintenance and Storage

The tracking (movement and location of records) will be managed by the Force Records Manager to ensure that any record can be:

- easily retrieved at any time;
- and that there is an auditable trail of record transactions.

The Force Records Manager will ensure appropriate environmental controls are provided for current records to prevent damage to the records.

The Force Records Manager will ensure equipment and facilities used for current records storage is fit for purpose and safe from unauthorised access, meeting fire regulations and providing reasonable protection from water, rodent or other damage, at the same time permitting maximum approved accessibility to the information and commensurate with its frequency of use.

A business continuity plan must be in place to provide protection for records which are vital to the continued functioning of the Force.

4. Review, Retention and Disposal

Please see Review, Retention and Disposal policy.

5. Access and Security

The legal and business environment in which the Force operates establishes broad principles on access rights, conditions and restrictions. All staff have a responsibility to ensure that records are classified and handled in accordance with this environment and are protected from unauthorised disclosure.

The Government's protective marking system (GPMS) applies to all Wiltshire Police records and information and will be complied with at all times.

The need to ensure appropriate access controls, both within Niche and in the wider force environments, will be managed by assigning access status to both records and individuals. Managing such access will ensure that:

- records are categorised according to their access status at a particular time;
- records are only released to those who are authorised to see them;
- encrypted records can be read as and when required and authorised;
- records processes and transactions are only undertaken by those authorised to perform them; and
- parts of the organisation with responsibility for particular business functions specify access permissions to records relating to their area of responsibility.

The monitoring and mapping of user permissions and role based functional job responsibilities is a continuing process which occurs in all records systems regardless of format. The data controller and business process owner will assign individuals access status in accordance with the FISP.

6. Training

The Force will ensure that all staff receive appropriate and timely training based on training needs analysis, using appropriate training products and a Force training needs analysis will be conducted at regular and appropriate intervals according to need.

The Force training needs analysis triggers will include:

- movement in staff at any level;
- change in functions and responsibilities, policy and/or principles;
- introduction of a new system(s);
- change in national or legislative records management environment.

The Force Records Manager will be responsible for conducting and recommending records management training needs analyses for each business area.

The Learning and Development Department will be responsible for co-ordinating, reviewing and recording training activities.

7. Audit and Compliance

Where an internal Force audit or quality assurance (QA) review is conducted, compliance with the Force records management policy and MoPI Code of Practice and Guidance will be included as an integral part of the review process.

The requirement to undertake annual inspections and quality assurance audits of business areas carried out independently of staff working within these environments is an integral part of MOPI and must be seen as being an important milestone to measure performance.

Audit trails will be provided for all records and documents. They should be kept securely and should be available for inspection by authorised personnel.

Audit trails will be managed since they may be of critical importance to the organisation. Claims of compliance may be discredited if the audit trail is not treated correctly and cannot be interpreted unambiguously.

The audit trail will include a record of all relevant occurrences and will be secure. If any significant occurrence is not audited, then the whole audit trail can be discredited and as a direct result all or any information held within the system will also be able to be discredited. For all audit trail data, it will be possible to identify the processes, enabling technology and individuals involved and the time and date of the event.

APPENDIX 1 - GLOSSARY

(Sourced from: Freedom of Information Act 2000 Model action plan for achieving compliance with the Lord Chancellor's code of practice on the management of records [3]. Model action plan for higher and further education organisations. V.2. 24 April 2002. pp. 15-18.
National Archives of Scotland. Glossary of Records Management Terms.
http://www.nas.gov.uk/reckeep/Glossary.asp)

Access	The availability of, or permission to consult, records.
Accountability	The principle that organisations and individuals are required to account to others for their actions. Government departments and agencies must be able to account for their actions to the appropriate regulatory authority.
Appraisal	The process of evaluating an organisation's activities and records to determine which records should be kept, and for how long, to meet the needs of the organisation, the requirements of Government accountability and the expectations of researchers and other users of the records.
Archive (n)	The physical place where archives are managed.
Authentic	An authentic record is one that can be proven to be what it purports to be, to have been created or sent by the person identified, and created or sent at the time purported. (BS ISO 15489: 2001)
Business recovery plan	A document which sets out the measures to be taken to minimise the risks and effects of disasters such as fire, flood, or earthquake, etc. and to recover, save and secure vital records should a disaster occur. It should include operational measures that enable the re-start of the business.
Classification system	The process of devising and applying schemes based on the business activities which generate records, whereby they are categorised in systematic and consistent ways to facilitate their capture, retrieval, maintenance and disposal. Classification includes determining document or file naming conventions, user permissions and security restrictions on records. (BS ISO 15489: 2001) In broad terms it is the process by which records are

	categorised or grouped into retrieval units, whether by function, subject, or other criteria.
Client manager	An officer of the Public Record Office responsible for giving advice and guidance to a group of government departments and agencies, to provide for the timely and effective appraisal, documentation and accessioning of departmental records.
Compliance	Fulfilling legal and regulatory requirements.
Current Records	Records necessary for conducting the current business of an organisation.
Data controller	This is the person (an individual or a corporate entity such as a company) who determines why, as well as how, personal data are to be processed. It is their duty to ensure that the collection and processing of any personal data within the organisation complies with the data protection principles.
Data processor	This is any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Data processors must have a written contract in which the data controller defines how personal data, including sensitive personal data, is to be processed and what security measures will be appropriate. Although the data processor must, of course, observe the terms of the contract, the data controller retains full responsibility for the actions of the data processor.
Data processing	The systematic performance of operations upon data (facts without structure or context) such as handling, merging, sorting, and computing; refers specifically to processing business data.
Data subject	The person who is the subject of the personal data. To count as a data subject the person must be living and capable of being identified from the data or other data in or likely to come into the possession of the data controller.
Digital	When applied to information, documents, etc. - information stored in a form, based not on human readable symbols but on a binary encoding, which can be manipulated by computers (and thereby made readable by humans).
Disposal	The implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive

	institution). They may also include the movement of records from one system to another (for example paper to electronic).
Disposition	A range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments.
Document	A structured unit of recorded information, published or unpublished, in hard copy or electronic form, and managed as a discrete unit. (BS ISO 15489:2001) A document becomes a record when it forms part of a business transaction and is linked to other documents relating to that transaction or process.
Documentation	Facts about a record keeping system, including its component parts and a manual of instruction detailing rules for use and maintenance of the system.
Electronic records	Records where the information is recorded in a form that is suitable for retrieval, processing and communication by a digital computer.
File	An organised unit of records, accumulated during current use and kept together because they deal with the same subject, activity or transaction.
Historical record	Anything recorded prior to the date that the MoPI Manual of Guidance comes into effect.
Information Survey	A comprehensive gathering of information about records created or processed by an organization.
Integrity	The quality which when present means that the record possesses a verifiably incorruptible data/content and can identify the intellectual qualities of information that make it authentic.
Life cycle	An approach to viewing the records management through a lifecycle model. It divides the record five major phases of existence - creation, distribution, use, maintenance and disposal. As part of the disposal it may enter into the archive or be destroyed.
Metadata	Descriptive and technical documentation to enable the system and the records (that are described) to be understood and to be operated efficiently, and to provide an administrative context for the effective management of the records.
Microform	Records in the form of microfilm or microfiche, including aperture cards.

Migration	In this context, it refers to the movement of data from one medium, or system, to another while maintaining the records' authenticity, integrity, reliability and usability.
Operational area	A unit, division or department within a government department or agency with responsibility for a particular function.
Paper records	Records in the form of files, volumes, folders, bundles, maps, plans, charts, etc.
Personal data	Factual information and expressions of opinion about, and any indications of anyone's intentions in respect of, living individuals who can be identified from that data or other data in the possession of, or likely to come into the possession of, the Data Controller. There are five categories of personal data: **Category (a)** Information being processed by means of equipment operating in response to instructions given for that purpose, for example a database or a system with search capabilities which enables information about individuals to be identified and retrieved **Category (b)** Information recorded with the intention of being so processed **Category (c)** Information that is not processed automatically but is recorded as part of a "relevant filing system" or with the intention that it should form part of a relevant filing system. A relevant filing system is one in which particular information about specific individuals can be readily retrieved. The internal structure of the files is therefore relevant. Any system whose primary purpose is to hold information about individuals and comprises files with an internal structure or referencing system that facilitates retrieval of specific information about those individuals falls within this definition. **Category (d)** Records relating to health, education, social work and housing that were previously subject to data subject access under other legislation. There is a statutory definition at section 68. **Category (e)** Recorded personal information that does not fall into any of the above categories and is held by a public authority

	as defined by the FOI Acts (see Schedule I) or a publicly owned company (Section 5 of the UK FOI Act and section 6 of the Scottish FOI Act). This category divides into two sub-categories: ○ **Semi-structured data**. This is data that is part of, or is intended to be part of, a set of information relating to individuals and that is structured by reference to individuals or by criteria relating to individuals but that does not have an internal structure or referencing system that would facilitate retrieval of specific information about particular individuals. An example would be a set of case files with a chronological arrangement of papers within each file. ○ **Unstructured data**. This is data that does not have the type of structure described above. An example would be a policy or subject file in which details of an individual occurred randomly.
Public records	Records of, or held in, any department of Her Majesty's Government in the United Kingdom or records of any office, commission or other body or establishment whatsoever under Her Majesty's Government in the United Kingdom, as defined in paragraph 2 of the First Schedule to the Public Records Act 1958. Also records of organisations subsequently included in the table in the above schedule or of those whose records have since been determined as public records by the Public Record Office.
Record	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. (BS ISO 15489: 2001)
Record Keeping System	An information system which captures, manages and provides access to records through time.
Records management	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (BS ISO 15489: 2001)

Record Officer	The person appointed by a government department or agency to be responsible for the management of the records of that organisation.
Registration	The act of giving a record a unique identifier on its entry into a record keeping system.
Retention	The continued storage and maintenance of records for as long as they are required by the creating or holding organisation until their disposal, according to their administrative, legal, financial and historical evaluation.
Retention schedule	A means to enable records managers to dispose of records promptly, consistent with effective and efficient operations, when the appropriate period of retention has expired.
Review	The examination of records to determine whether they should be destroyed, retained for a further period, transferred to an archival establishment, or presented to a third party.
Semi-current records	Records which are no longer required for the conduct of current business and which are waiting to be appraised for their long-term value or disposed of in accordance with disposal schedules.
Survey	An examination of current and semi-current records noting briefly their nature, systems of arrangement, date ranges, quantities, function, physical condition, reference activity and rates of accumulation.
Version control	A process that allows for the precise placing of individual versions of documents within a continuum.
Vital records	Those records that are essential to the operation of the organisation, the continuation and/or resumption of operations following a disaster. The recreation of legal, regulatory or financial status of the organisation, or to the fulfilment of its obligations, in the event of a disaster.