

NOT PROTECTIVELY MARKED

Force Procedure No: 166/P

Replaces Force Procedure:

Procedure Owner: **Records Manager  
Information Management and  
Technology**

Date Procedure Approved: 17/09/07

Date Procedure Last Revised: 09/09/08

Reviewed: 07/08/09



# FORCE PROCEDURE:

## Records Management

This document should be read in conjunction with the Records Management Policy.

*This procedure has been drafted in accordance with the Human Rights Act 1998, Race Relations (Amendment) Act 2000 and the principles underpinning it. It is suitable for public disclosure*



## Records Management Procedures

### **1. ABOUT THIS PROCEDURE**

- 1.1 These procedures will be incrementally adopted by the Force as the framework for implementing Records Management processes into the Force by 2010. Implementation will be achieved through an Action Plan managed within the Information Management programme.
- 1.2 As processes are changed or introduced, this document will be amended to incorporate the procedures adopted.
- 1.3 The procedures have been written to ensure all aspects of the Management of Police Information (MoPI) Code of Practice (CoP) 2005 and Guidance 2006 requirements will in due course be adopted into business as usual within the Force.

### **2. RISK ASSESSMENTS / HEALTH & SAFETY CONSIDERATIONS**

- 2.1 There is an inherent risk to the Force through litigation if records are not managed in an appropriate manner. Adherence to the Records Management Policy and Procedures will reduce the risk to the force.
- 2.2 There is a risk of damage to the Forces reputation if it does not comply with Data Protection (DP) and Freedom of Information (FOI) requests due to mismanagement of records
- 2.3 There is a risk with the physical storage of records – damage caused to records due to damp, flood, fire, rodents etc. Also the physical security of records which should be stored in line with Government Protective Marking Scheme (GPMS) ensuring authorised access only.
- 2.4 Risk Assessments including Health and Safety Assessments will be carried out to identify risks to staff by the appropriate line manager.
- 2.5 It is essential that Divisions and Departments identify vital records within their Business Continuity Plans. This will reduce the risk of not being able to continue with the business of running West Mercia Constabulary.

### **3. PROCEDURE**

#### **3.1 Key Principles**

- 3.1.1 To ensure that Force records are complete, reliable, authentic, secure and accessible, the following principles will be followed:
  - i) Records will be categorised in accordance with the Force filing system ie Q drive, which should align to the Police Service File Plan (PSFP).

## Records Management Procedures

- ii) Records will be stored so as to provide adequate protection against unauthorised access or damage.
- iii) Records will be readily available to meet operational, business need and legal obligations.
- iv) Records will be disposed of in accordance with the Retention/Disposal Schedule and an audit trail kept.
- v) Records management systems will provide an auditable trail of record transactions from creation through to ultimate disposal.
- vi) Divisional/departmental compliance with this policy will be reviewed as part of Performance Management.

### **3.2 Records Management**

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

#### **3.2.2 Authenticity**

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

#### **3.2.3 Accuracy**

Records will be accurate.

#### **3.2.4 Integrity**

Records will be securely maintained to prevent unauthorised access, alteration, damage, or removal. Records will be Government Protective Marking Scheme (GPMS) marked and 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 record preserved remains authentic and accurate.

#### **3.2.5 Usability**

Records will be readily available This includes the accessibility and use of electronic records for as long as is required and the ability to cross reference electronic records to their paper counterparts in a mixed environment.

### **3.3 Record Creation**

3.3.1 The Force will have in place controls to ensure the record is created on the appropriate form or database and is assigned the relevant classification, naming convention and protective marking.

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

## Records Management Procedures

3.3.3 Records will be created in line with MoPI Guidance, in particular when recording information Managers/Supervisors will ensure compliance with Checklist 1 of the MoPI Guidance.

3.3.4 Person records will only be created if the minimum requirement set down by the MoPI Guidance can be complied with.

### **3.4 Evaluation of Information**

3.4.1 Information will be subject to an evaluation line with MoPI Guidance.

3.4.2 Information should be evaluated to determine the reliability and the credibility of the source, and the value and content of the information.

3.4.3 Evaluation should be proportionate to the nature of the information.

### **3.5 Registration**

3.5.1 All records, must be maintained in an approved filing structure that will include

- i) A unique identifier assigned from the system/register
- ii) The date and time of registration
- iii) A title or abbreviated description
- iv) The author, sender or recipient

3.5.2 In a manual system the register will be a separate record, in electronic systems the register will be incorporated into the system. The register should be unalterable and auditable.

3.5.3 Managers/Supervisors will be responsible for ensuring that all registered files are available for those with authorised access.

3.5.4 Files will remain on the register in line with MoPI Guidance on review, retention and disposal.

### **3.6 Classification (File Plan)**

3.6.1 The Force will have in place a records classification scheme based on the business functions and activities that generate records. Records will be categorised in a systematic and consistent way to facilitate:

- i) Links between records that originate from the same activity or from related activities.
- ii) Retrieval of all records relating to a particular function or activity.
- iii) Assessment of security protection and appropriate access for sets of records.
- iv) Distribution of responsibility for management of particular sets of records.
- v) Evaluation of appropriate retention/review periods for records

3.6.2 The use of a functional based classification scheme will reduce the need for changes within the file plan if future reorganisation of divisions/departments takes place.

## Records Management Procedures

3.6.3 Any classification scheme introduced within West Mercia Constabulary will align to the Police Service File Plan (PSFP) as recommended by MoPI Guidance.

### **3.7 Metadata**

3.7.1 All records will contain, be linked to or associated with, metadata – this is descriptive and technical information about the file or document such as:

- i) How, when, and by whom it was received, created, accessed, and/or modified and how it is formatted.
- ii) The intended review/disposal date of electronic records should be included in the metadata when the record is created.

### **3.8 Records Maintenance and Storage**

3.8.1 The Force will implement a tracking system for physical records that enables the user to

- i) Establish the presence or absence of information on a given subject.
- ii) Identify and locate relevant information within a set of records.
- iii) Group together information on subjects.

3.8.2 The tracking (movement and location of records) system will be supervised by the Records Manager to ensure that any records can be:

- i) Easily retrieved at any time,
- ii) There is an auditable trail of record transactions

3.8.3 Equipment and facilities used for the records storage must be fit for purpose and safe from unauthorised access, meeting fire regulations and providing reasonable protection from water, rodent or other environmental damage.

3.8.4 The security of the storage must reflect the GPMS grading at the same time permitting maximum approved accessibility to the information and commensurate with its frequency of use.

3.8.5 A business continuity plan must be in place to provide protection for records which have been identified as being vital to the continued functioning of the Department the Division or the Force.

### **3.9 Disclosure and Dissemination**

3.9.1 Any information suitable for dissemination and/or disclosure will be dealt with in line with the force disclosure policy.

### **3.10 Review, Retention and Disposal**

3.10.1 The Force will implement a Review, Retention and Disposal (RRD) Policy in line with legislative and operational governance including Data Protection Act 1998, Limitation Act 1980, Criminal Procedures Investigation Act 1996 and MoPI Codes of Practice, Guidance and Threshold Standards.

## Records Management Procedures

3.10.2 The RRD Policy will ensure that information is lawfully held by the Force. This will also prevent the Force being overloaded by the volume of information captured and recorded.

3.10.3 Records which no longer have a policing purpose but which may have historical value may be archived for long term retention. It must be made clear that the records are kept for this purpose only.

### **3.11 Retention/Disposal Schedule**

3.11.1 The Force Retention Schedule will set out the review, retention and disposal periods for policing records held by the Force in line with legal, operational and business requirements and MoPI guidance. (This schedule has not yet been agreed.)

### **3.12 Access and Security**

3.12.1 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.

3.12.2 The Government Protective Marking Scheme (GPMS) applies to all Force records and information and will be complied with at all times. (Further information on GPMS can be found on the Intranet or from the Information Security Officers.)

3.12.3 Any access and/or security restrictions must be reviewed at appropriate intervals to ensure that the additional security controls required for these records are not enforced longer than required.

3.12.4 The business system owner will assign individuals access status in accordance with Force Information Security Policy (FISP). The monitoring and mapping of user permissions and functional job responsibility roles is a continual process and is defined within the System Accreditation under the Access Control Procedure.

3.12.5 Access to information will be restricted to appropriately vetted staff.

3.12.6 Any Information shared will be subject to the Force's Records Management Policy. The Force will always remain the owner of any information shared.

### **3.13 Training**

3.13.1 The Force will ensure all staff receive appropriate and timely training based on training needs analysis, using appropriate training products.

3.13.2 The Records Manager will liaise with the Head of Training and Development to ensure training needs are addressed.

3.13.3 The Head of Training and Development will be responsible for co-ordinating, and recording training activities.

## Records Management Procedures

### **3.14 Audit and Compliance**

- 3.14.1 Where an internal Force audit or quality assurance (QA) review is conducted, compliance with the Records Management Policy and Procedures will be included as an integral part of the review process.
- 3.14.2 Records Management Policy and Procedures will be audited in line with the Force Audit Policy
- 3.14.3 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 cannot be proved.

## **4 ROLES & RESPONSIBILITIES**

### **4.1 Information Management Strategy Group**

The Chief Constable has overall responsibility for West Mercia Constabulary's Records Management Policy and Procedures, and for supporting the application of the policy Force wide.

- 4.1.2 In addition to the responsibilities outlined in the Information Strategy (IMS), the Information Management Strategy Group will:-

- i) Ensure clear lines of accountability for records management
- ii) Monitor and review systems in place for records management at least annually in order to make improvements
- iii) Appoint a senior manager responsible for co-ordinating, publicising and monitoring implementation of the records management policy and reporting on a regular basis to the group.
- iv) Seek independent assurance that an appropriate and effective system of managing records is in place.

### **4.2 Records Manager**

- 4.2.1 The Records Manager is responsible for the co-ordination of Records Management within the Force, as defined within the IMS

### **4.3 Senior Management (Business System Owners)**

- 4.3.1 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 will be determined by the Records Manager for disposal purposes.

- 4.3.2 The responsibilities for Senior Management (Business System Owners) are outlined in the IMS

### **4.4 Supervisors or Equivalent (day to day maintenance, Monitoring)**

- 4.4.1 Each business area will have a designated supervisor with responsibility for:
- i) The development, operation and communication of approved records management procedures, covering both electronic and hard copy media.

## Records Management Procedures

- ii) Ensuring records are fit for purpose and in the appropriate recording format.
- iii) Ensuring information is recorded for a policing purpose and complies with the Records Management Policy and Procedures
- iv) Quality assurance of records management processes and procedures.
- v) Ensuring that staff are aware of their personal responsibilities for record keeping.
- vi) Provide feedback to staff with regard to their record keeping, where required.
- vii) Ensuring staff training is provided that is appropriate to maintaining a high standard of skills and competence..
- viii) Ensure the timely submission of information to the Force.
- ix) Fulfil their responsibilities in relation to recording, evaluation, sharing and reviewing information in accordance with MoPI Guidance.

### **4.5 All Staff**

- 4.5.1 All staff involved in recording, evaluation, sharing and reviewing information will do so in accordance with their individual responsibilities as detailed in the IMS.

## **5 MONITORING / EVALUATION**

- 5.1.1 Effectiveness of the procedures contained in this document will be monitored and evaluated by the Records Manager.

## **6 REVIEW**

- 6.1 This document will be reviewed annually on the date of publication.

- 6.2 The review will consider:-

- Changes to general principles underpinning the policy
- Changes in the law that have an impact on the policy
- Issues from the monitoring and evaluation process
- Relevance of policy objectives
- Challenges to the policy by events/incidents/staff
- Adverse effects on other departments, staff groups, or any other person
- Identified inefficiencies in relation to the policy's implementation
- Policy/procedure communication

- 6.3 The policy to which this procedure applies is the Force Records Management Policy.

Records Management Procedures

**Records Management Glossary**

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. Divisions and departments must be able to account for their actions to the appropriate regulatory authority.
Archives	The physical place where records that have long term value are stored and/or 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 continuity plan	A document which sets out the measures to be taken to minimise the risks and effects of disasters such as fire or flood etc. and to recover, save and secure vital records should a disaster occur. It should include operational measures that enable the restart of the business.
Classification scheme	The process of devising and applying schemes based on the business functions and activities which generate records. This allows categorisation in a 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)
Compliance	Fulfilling legal and regulatory requirements.
Current records	Records necessary for conducting the current business of the Force.
Disposal/Destruction	Deletion or destruction of records in a way which they cannot be reconstructed by any commonly known means.
Document	A structured unit of recorded information, published or unpublished, in hard copy or electronic form, and managed as a discrete unit. (BSO 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.
Electronic records	Records where information is recorded in a form that is suitable for retrieval, processing and communication by 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 the MoPI Manual of Guidance came into effect. (31 March 2006)
Integrity	The quality which when present means that a record possesses a verifiably incorruptible data/content and can identify the intellectual qualities of information that make it authentic.

## Records Management Procedures

Lifecycle	An approach to viewing the records management through a lifecycle model. It divides the records 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 that details the author, time and date of creation, and if electronic, the format in which it was created.
Migration	In this context, it refers to the movement of data from one media or system to another i.e. paper to electronic, while maintaining the records authenticity, integrity, reliability and usability.
Operational/Business area	A unit, division or department within the Force with responsibility for a particular function.
Paper records	Records in the form of paper that make up files, volumes, folders, maps, plans, charts, etc.
Personal Data	Factual information and expression of opinion about any 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.
Records	Information created, received, and maintained as evidence and legal information by an organisation or person, in pursuance of legal obligations or in the transaction of business. (BS ISO 15489:2001)
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)
Records Manager	The person appointed by the Force to be responsible for the management of records within the Force.
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 the disposal 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 retained for a further period or be destroyed.
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.