Integrity | Professionalism | Fairness | Respect

• Records Management, Retention and Disposal Policy and Procedure

Reference No.	**P23:2013**

Implementation date	**15th July 2013**
Version Number	**V1.1**

Linked documents	
Reference No:	**Name.**
P23A:2013	Compliance with MoPI Section 7, Review, Retention and Disposal (RRD)
P23B:2013	MoPI RRD Standard Operating Process
P23E:2013	ACPO Retention Schedule

Suitable for Publication	
Policy Section	**Yes**
Procedure Section	**No**

Protective Marking
Protected

PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UP TO DATE VERSION CAN BE FOUND ON THE FORCE INTRANET POLICIES SITE.

Table of Contents

1 Policy Section

1.1 Statement of Intent – Aim and Rationale

This policy defines a framework for managing Dorset Police (hereafter referred to as the force) records including their retention and disposal. Its aims are to:

- Establish good records management practices throughout the force;
- Ensure that force records are managed appropriately throughout their life, in the formats that most suit their requirements;
- Provide the basis for building the forces corporate memory;
- Support the force in demonstrating accountability to its stakeholders and protecting the legal and moral rights of its customers and any persons affected by its actions;
- Gain recognition of records management as a corporate function with sufficient levels of support in order to be effective;
- Define roles and responsibilities;
- Promote compliance with information related legislation and codes of practice.

1.1.1 Applicability

This policy applies to all categories of force employees, including full-time, part-time, fixed term, permanent and seconded staff. It also applies to Police Officers and Police Staff, temporary and agency staff, Volunteers, Specials and Modern Apprentices, who will collectively be referred to as 'employees' for the purpose of this policy.

1.2 Our Visions and Values

Dorset Police is committed to the principles of "One Team, One Vision" – A Safer Dorset for You"

Our strategic priority is to achieve two clear objectives:

- To Make Dorset Safer
- To Make Dorset Feel Safer

In doing this we will act in accordance with Our Values of:

- Integrity
- Professionalism
- Fairness and
- Respect

National Decision Model

The National Decision Model (NDM) is the primary decision-making model used in Dorset Police. The NDM is inherently flexible and is applied to the development and review of all policy, procedure, strategy, project, plan or guidance. Understanding, using and measuring the NDM ensures that we are able to make ethical (see Code of Ethics), proportionate and defensible decisions in relation to policy, procedure, strategy, project, plan or guidance.

Code of Ethics

The Code of Ethics underpins every day policy, procedures, decision and action in policing today. The Code of Ethics is an everyday business consideration. This document has been developed with the Code of Ethics at the heart ensuring consideration of the 9 Policing principles and the 10 standards of professional behaviour. Monitoring is carried out through the Equality Impact Assessment process which has been designed to specifically include the Code of Ethics.

1.3 People, Confidence and Equality

This document seeks to achieve the Priority to Make Dorset Feel Safer by Securing Trust and Confidence. Research identifies that this is achieved through delivering services which:

1. Address individual needs and expectations
2. Improve perceptions of order and community cohesion
3. Focus on community priorities
4. Demonstrate professionalism
5. Express Force values
6. Instil confidence in staff

This document also recognises that some people will be part of many communities defined by different characteristics. It is probable that all people share common needs and expectations whilst at the same time everyone is different.

Comprehensive consultation and surveying has identified a common need and expectation for communities in Dorset to be:-

- Listened to
- Kept informed
- Protected, and
- Supported

2 Standards

2.1 Legal Basis

The force is committed to complying with the laws related to information and records management, in addition to the following best practice guidance and relevant codes of practice.

2.2 People, Confidence and Equality Impact Assessment

During the creation of this document, this business area is subject to an assessment process entitled “People, Confidence and Equality Impact Assessment (EIA)”. Its aim is to establish the impact of the business area on all people and to also ensure that it complies with the requirements imposed by a range of legislation.

2.3 Monitoring / Feedback

This policy is owned by the Head of Professional Standards. Any queries regarding the policy content should be directed in the first instance to the Records Management Supervisor by email to .FISU Records Management Supervision

The Policy Co-ordinator can be contacted in relation to any policy issues by email to .Policies

This policy will be monitored by the Force Information Standards Manager.

- The Force is assessed by ACPO on compliance with MoPI Codes of Practice
- Data Protection will conduct internal audits to ensure compliance with MoPI Codes of Practice.
- Dorset Police has adopted the ACPO National Retention Schedule, variations to the schedule are by exception only and must be agreed by the Information Management Board (IMB).

Departmental and Divisional leads will be identified to audit and monitor records within their business area.

Feedback relating to this policy can be made in writing or by e-mail to
Address: Force Information Standards Manager, Dorset Police Headquarters, Winfrith, Dorchester, DT2 8DZ
E-mail: rmsupervision@dorset.pnn.police.uk
Telephone: 01202-22 3492

3 Procedure Section

A Glossary of Terms can be found at Appendix A.

3.1 Scope

This policy applies to all the existing, and any planned force collections throughout their lifecycle, regardless of record format, medium, physical location or age. It also applies to records created, held or maintained within structured information systems or databases. It does not apply to records held by the Home Office on national information systems such as PNC and PENTIP.

3.2 Context

This policy has been written in accordance with the Code of Practice under S46 of the Freedom of Information Act (hereafter known as the S46 Code of Practice) and seeks to achieve compliance with this code. It also seeks to facilitate compliance with the other relevant information-related legislation, codes of practice and regulations. This policy also takes into account best practice guidance issued by the National Archives and other internationally recognised expertise in this field.

This policy is supported by a Records Retention Schedule and a series of related procedures, instructions and guidance for organisational best practice. These do not form part of the policy but will be regularly updated to cater for any changes taking place within the force or nationally.

3.3 Policy Statement

The Force will adopt the following as the framework for managing it records:

3.3.1 The Force will recognise Records Management as a corporate responsibility and is committed to providing the required organisational support in order to ensure its effectiveness. The force's records are a major component of its corporate memory and as such are vital assets that support ongoing operations and business continuity as well as providing valuable evidence or business activities over time.

3.3.2 The Force will ensure records can be captured, identified and retrieved when required by providing well-structured processes, procedures and guidance.

3.3.3 The final decision as to which documents become records lies with the business units and individuals responsible for the activities resulting in the creation of those documents. Such a decision depends on the significance of the information to those activities.

3.3.4 The Forces records of its business activities will be as complete, accurate, authentic, reliable and usable as possible.

3.3.5 The Force will safeguard its records from unauthorised alteration, degradation or unscheduled destruction, regardless of record format.

3.3.6 The Force will ensure the identification of those records that are deemed as vital to the continued functioning of the organisation, putting in place contingency or business recovery plans for their protection, throughout the period for which they are required.

3.3.7 The Force will ensure that its records are stored, handled and managed securely throughout their life, according to their security markings and in accordance with the Government Protective Marking Scheme and Information Security Policy.

3.3.8 The Force will ensure that its records are closed as soon as they are no longer in active use, other than for informational or reference purposes.

3.3.9 The Force will ensure that its closed records remain available and accessible to those with authorised access.

3.3.10 The Force will have in place a Records Retention Schedule, containing retention timescales established in accordance with legislative, statutory and regulator requirements, recognised best practice and business requirements. The force will retain and dispose of its records in accordance with that schedule.

3.3.11 The disposal of records, regardless of format will be undertaken only by the authorised personnel, in a manner consistent with their protective marking and any other applicable force policies.

3.3.12 The Force will ensure that where back-ups, copies and renditions of records exist, their retention and disposal is managed in accordance with the original source records which they support.

3.3.13 The Force will ensure that where records are scheduled for destruction in accordance with the force Records Retention Schedule, their scheduled destruction is carried out securely and in such a way that prevents any subsequent recovery by any employee.

3.3.14 The Force will ensure the timely and effective appraisal of its closed records and transfer those deemed worthy of permanent preservation, to the County Archives.

3.3.15 Any decision regarding the disposal of records (including destruction, reviewing for further retention or transfer to the County Archives) following expiry of their retention periods shall be made in consultation with the business unit responsible for the activities through which the records were created.

3.3.16 The Force will manage its records according to business functions and activities and will review, retain and dispose of records as per the Records Retention Schedule.

3.3.17 The Force will comply with all relevant legislation (see section 3.5) with regards to the management of its records. Force records that are identified as falling within the scope of 'police information' as defined in the Code of Practice on the Management of Police Information as associated guidance will be reviewed, retained and disposed on in accordance with that Code. The force will provide employees with records management guidance and awareness, and as well as giving guidance on the creation of accurate and reliable records, will draw attention to the implications of not creating adequate records.

3.4 Roles and Responsibilities

The Force has a corporate responsibility to maintain its records and records management systems in accordance with the regulatory environment. All force employees have a responsibility to capture the records that they produce in the execution of their duties. To support them in the management of these records the following roles and responsibilities have been identified:

3.4.1 Data Controller

The Chief Constable, as Data Controller, has overall responsibility for the force's compliance with the MoPI Code of Practice and other legislation relevant to records management. The Data Protection Act 1998 also places a legal obligation on the data controller to comply with the act, which applies to all "personal data" meaning data which relates to a living individual. The data controller owns the Information Management Strategy (IMS) and has responsibility for ensuring that force policies and processes comply with this guidance.

3.4.2 Senior Information Risk Owner (SIRO)

The Deputy Chief Constable (DCC) is the force SIRO. The SIRO has responsibility for understanding how the strategic business goals of the Force may be impacted by information management systems failure and is responsible for ensuring that information risk management and management processes are established and adhered to Force-wide. This is a strategic responsibility, which will not be confined to information technology or information assurance departments.

3.4.3 Chief Information Officer (CIO)

The Head of Professional Standards is also the CIO, and as such has responsibility for strategic direction and oversight, being sufficiently senior to act as the accountable person and a champion for records management. This person oversees policy and strategy and ensures that the necessary resources are made available and remedial action is taken when problems arise.

3.4.4 Force Information Standards Manager

The Force Information Standards Manager is a member of the Information Management Board and chairs the Information Management Working Group, reporting to the Chief Information Officer they have senior-level responsibility for the Management of Police information, including records management.

3.4.5 Records Management Supervisor

The Records Management Supervisor has operational responsibility for records management at practitioner level; they develop the records management programme and then manage its implementation and overall functioning. They are authorised to dispose of records in accordance with policy and procedures. They have supervisory responsibility for review staff and archive officers and report to the Force Information Standards Manager.

3.4.6 Information Security Officer and Assurance Manager

The Information Security Officer and Assurance Manager ensures that arrangements within force for managing police information include procedures and technical measures to prevent unauthorised or accidental access to, amendment of, or loss of police information. They are also responsible for Data Protection, Freedom of Information and Computer Systems Audit.

3.4.7 Head of Information Systems

The Head of Information Systems is responsible for enabling the delivery and development of a records management capability through the provision of the supporting IT infrastructure, tools and technical support to users.

3.4.8 Sharepoint Administrators

Sharepoint Administrators must be appointed within each Command/business area, to act as local champions. They will act as the local point of contact for the records management team and will be responsible for ensuring that records are managed on Sharepoint in accordance with policy and guidance. The Force Information Standards Manager will ensure that the appropriate level of training is provided. Administrators are a self supporting group who meet when required to identify solutions to problems and promote best practice.

3.4.9 Information Technical Training Officer

The Information Technical Training Officer will prepare guidance on managing records on Sharepoint for Sharepoint administrators and will assist the Force Information Standards Manager by providing training to them when required.

3.4.10 Heads of Department

Heads of Departments and business area managers are responsible for ensuring that their staff keep adequate records of their work in accordance with agreed procedures and arrangements. Managers should ensure that all police information is managed in compliance with the Management of Police Information Code of Practice 2005 and the Data Protection Act 1998. All records should have the correct GPMS/GSC marking and be stored in the appropriate format. Managers are responsible for authorising the disposal of any information by their staff and ensuring that policies and guidance are adhered to.

3.4.11 All employees

All employees involved in the process of collecting, recording, evaluating, sharing, disseminating, reviewing and disposing of police information are responsible for ensuring that they comply with the data quality principles of the Data Protection Act 1998.

There are key principles which apply, regardless of the format and business area where police information is held. The person recording the information must ensure that they have regard to these principles.

- A record must have been created for a policing purpose
- All Records must comply with the Data Quality Principles
- A record of police information is the start of an audit trail and must identify who completed the record, when it was completed and for what purpose

- Before recording information, checks should be made in other business areas to see whether this information is already held; this will help avoid unnecessary duplication.
- If information is recorded on an individual who is the subject of an existing record, the record should reflect this
- If it becomes apparent that the information being recorded is connected to other information, it must be appropriately linked
- Police information must be recorded as soon as it is practicable in accordance with the standards relating to the business area in which the information is held
- Consideration should be given to the application of the appropriate Government Security Classification (GSC).
- Where appropriate the source of the information should be recorded to ensure accuracy and to assist in request for further information.

3.5 Boards and Working Groups

3.5.1 Information Management Board (IMB)

The IMB is chaired by the SIRO and meets on a quarterly basis. It deals with strategic issues surrounding information management. The IMB will determine the organisation's policy for information assets and identify how compliance with that policy will be measured and reviewed. The IMB will oversee the implementation and maintenance of the Information Management Strategy.

3.5.2 Information Management Working Group (IMWG)

The IMWG is chaired by the Force Information Standards Manager and meets on a quarterly basis. It deals with information management at practitioner level. Policies and procedures are routed through the working group prior to submission to the IMB.

3.5.3 Sharepoint Administrators User Group

The Sharepoint Administrator's User Group meets on a need only basis for the purpose of resolving issues and promulgating best practice in the area of records management on Sharepoint. The user group is chaired by the Force Information Standards Manager and reports to the IMWG.

3.6 Legislation and Standards

The force is committed to complying with the laws related to information and records management, in addition to the following best practice guidance and relevant codes of practice.

The following have been identified as relevant and applicable to the force and the records management implications of these have been considered within the scope of this policy.

3.6.1 Legislation

- Regulation of Investigatory Powers Act 2000
- Criminal Procedure and Investigation Act 1996
- The Public Records Acts of 1958 and 1967
- Freedom of Information Act 2000
- Data Protection Act 1998
- Human Rights Act 1998
- Limitations Act 1980
- Health and Safety at Work etc Act 1974
- Environmental Information Regulations 2004
- Protection of Freedoms Act 2012

3.6.2 British Standards (BSI)

The force will consider the following standards in its records management practices:

- BS 4783 Storage, transportation and maintenance of media for use in data processing and information storage.
- BS ISO 9001:2008 – Quality management systems.
- BS ISO/IEC 17799:2005 – British and International Standard – Code of Practice for Information Security Management
- BS ISO/IEC 27001:2005 – Information technology. Security techniques. Information security management systems. Requirements.
- BS ISO 15489-1:2001 – Information and documentation. Records management. General.
- PD ISO/TR 15489-2:2001 – Information and documentation. Records management. Guidelines.
- BIP 0008-1:2004 – Code of Practice for legal admissibility & evidential weight of Information stored electronically.
- BS 10008:2008 – Evidential weight and legal admissibility of electronic information. Specification.
- BIP 0008-2:2005 – Code of Practice for legal admissibility & evidential weight of Information communicated electronically.
- BIP 0008-3:2005 – Code of Practice for legal admissibility & evidential weight of linking electronic identity to documents.
- BSI DISC PD0010 – Principles of good practice for information management.

3.6.3 Codes of Practice

- The Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000
- Code of Practice on the Management of Police Information 2005

3.6.4 The National Archives Standards

The National Archives publishes standards, guidance and toolkits on the management of public records in all formats, covering their entire lifecycle. They are available on The National Archives website: http://www.nationalarchives.gov.uk

3.6.5 Further Information

For further information regarding information and records management, please access the following external resources:

- http://www.ico.gov.uk/
- http://www.nationalarchives.gov.uk/

3.7 Implications of the Policy and Procedure

3.7.1 Training Requirements

All employees need to understand their responsibilities to create and manage records of their business activities. In accordance with S46 Code of Practice, the force has in place a professional development programme for employees with records management duties.

The maintenance and disposal of records is the responsibility of the Records Management Team and will be carried out in consultation with Heads of Department and Business Area Managers.

3.7.2 IT Infrastructure

The force's current records management capability is achieved using the Force-wide system, NICHE RMS and standard Microsoft Windows and Office based functionality including Sharepoint.

3.7.3 Related Policies

In addition, this policy is supported by the following additional policies and documentation:

- ACPO Retention Schedule
- Compliance with MoPI Section Seven
- Information Security Policy
- Data Protection Policy
- Business Continuity Management Policy
- Internal Communication Policy
- Internet Access and Email Use Policy
- Information Sharing Policy

3.8 Monitoring

3.8.1 Monitoring

Compliance with this policy will be regularly monitored. Following established procedures, monitoring activities will be carried out by Information Security and Assurance, Professional Standards.

Such reviews will examine organisational performance and user satisfaction with the system.

Modification to the records systems and record management processes will be made if these are found to be unsuitable or ineffective.

Systems compliance and monitoring will be documented and reports will be maintained and published across the organisation on a regular basis.

The Force Information Standards Manager and Records Management Team will monitor the effectiveness of the records retention content and the related Records Retention Schedule to ensure their respective relevance and fitness for purpose and to ensure that they are consistent with current legislation, codes of practice and industry best practice.

3.8.2 Policy Review and Audit

The Force Information Standards Unit will review this policy every year, or earlier if required to maintain its relevance, fitness for purpose and ensure it is consistent with current legislation, codes of practice, industry best practice and any internal changes to the organisation.

The force will monitor compliance with this policy by regular review and sampling in order to:

- Identify areas of operation that are not covered by the policy
- Highlight where non-conformance to the supporting procedures is occurring and suggest a tightening of controls and adjustment to related procedures such as security access.
- Identify any procedures or guidance which require updating or development, to ensure their consistency with, and adherence to, the policy.

The force will develop a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of electronic records. This will involve reporting any recommended modifications to the IMB.

4 Consultation and Authorisation

4.1 Consultation

Version No:	Name	Signature	Date
Police & Crime Commissioner			
Police Federation			
Superintendents Association			
UNISON			
Other Relevant Partners (if applicable)			

4.2 Authorisation of this version

Version No: 1.1	Name	Signature	Date
Prepared:	Jodi Twist		23/06/14
Quality assured:	Karen Elliott		15/07/14
Authorised:	Superintendent Dave Thorp		30.1.14
Approved:			

.

5 Version Control

5.1 Review

Date of next scheduled review	**Date: 3rd September 2015**

5.2 Version History

Version	Date	Reason for Change	Created / Amended by
1.0	June 2013	New policy/procedure updated to replace P10:2009 and P06:2010	K Elliott
1.1	July 2014	Annual review and updated linked documents	K Elliott

5.3 Related Forms

Force Ref. No.	Title / Name	Version No.	Review Date

5.4 Document History

Present Portfolio Holder	Deputy Chief Constable
Present Document Owner	Head of Professional Standards
Present Owning Department	Professional Standards
Details only required for version 1.0 and any major amendment ie 2.0 or 3.0:	
Name of Board:	Information Management Board
Date Approved:	11 July 2013
Chief Officer Approving:	DCC J Vaughan

Template version January 2013

APPENDIX A

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. 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	A collection of historical documents or records providing information about a place, institution, or group of people. Or to Place or store (something) in such a collection.
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.
Compliance	Fulfilling legal and regulatory requirements.
Current Records	Records necessary for conducting the current business of an organisation.
Data	Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analogue quantities to which meaning is or might be assigned.
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 processing	The systematic performance of 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.
Destruction	Process of eliminating or deleting records, beyond any possible reconstruction.
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.
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.
Paper records	Records in the form of files, volumes, folders, bundles, maps, plans, charts, etc.
Personal data	Data which relate to a living individual who can be identified— (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;
Preservation	Process and operations involved in ensuring the technical and intellectual survival of authentic records through time.
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 that 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)
Records 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.
Tracking	Creating, capturing and maintaining information about the movement and use of records.
Transfer (custody)	Change of custody, ownership and/or responsibility for records.
Transfer (movement)	Moving records from one location to another.
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.