Guidelines for Developing an Information and Records Management Policy

By Patrick Lambe and Marita Keenan

This set of guidelines is intended (i) to help an organisation understand the complementary relationships between knowledge management, information management, and records management; (ii) to structure a policy development exercise so that policies affecting the flow and use of knowledge, information and records are mutually supportive and are aligned towards improving organisational effectiveness.

The guidelines focus in particular on information and records management as enablers of knowledge management, and do not capture all aspects of knowledge management needs. Knowledge management includes management practices in relation to both tangible information artefacts such as documents and records, as well as to more intangible knowledge assets such as experience, skills, and ways of doing things.

The intangible aspects of knowledge management are less directly influenced by policy work, which is designed to govern the management of tangible practices, processes and artefacts. However, the policy environment that relates to information and records has a strong impact on the ability of people to access and use their knowledge resources effectively, and to this extent, it has a high relevance to the capture, access and use dimensions of knowledge management.

1. Definitions

1.1 Information and Information Management

We define “information” as codified knowledge which is transferred and stored by means of documents, records, publications, databases, tools, images, plans, sound/video recordings etc. In these guidelines we use the term “document” to refer to any of the forms in which information is carried.

For the purposes of this paper we define “information management” as the discipline of effective creation, collection, storage, access, use and disposal of information assets. “Disposal” does not necessarily mean destruction. It can mean transition to inactive or archival status. “Archival status” does not simply mean storing information (or in the instance of data, moving it off-line). It means the designation of particular sets of information as having enduring value either to the organisation or to wider society. As such managing the information as an archive is based upon special guidelines and policies which for public agencies are normally issued by government bodies, such as a national archive or a national library, in that jurisdiction.

Information management is an important component of **organisational effectiveness**, which we define as:

- the ability to set and achieve organisational goals within target timeframes at a competitive cost and effort;

- the ability to respond appropriately to emerging risks and opportunities in the environment.

Information management supports organisational effectiveness by providing:

- **Consistency** of information - especially in customer facing processes
- **Coordination** between business units - especially for minimising errors
- **Control** of business activities - for ensuring timely and relevant decisions
- **Compliance** with laws, regulations, policies, standards and accreditation requirements - for ensuring accountability
- **Cost Control** - for avoiding re-work and redundancy of resource and effort

When we assess the information management policies, procedures and practices, we are also assessing whether they are able to capture and manage the characteristics of information through its life cycle from creation, to use, to disposal.

1.2 Records and Records Management

"Records" form a sub-set of information, and because the discipline of "records management" is driven by regulatory and accountability requirements, its practices are much more clearly defined.

"Records" are defined as follows:

> **ISO 15489**
> 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.[1]

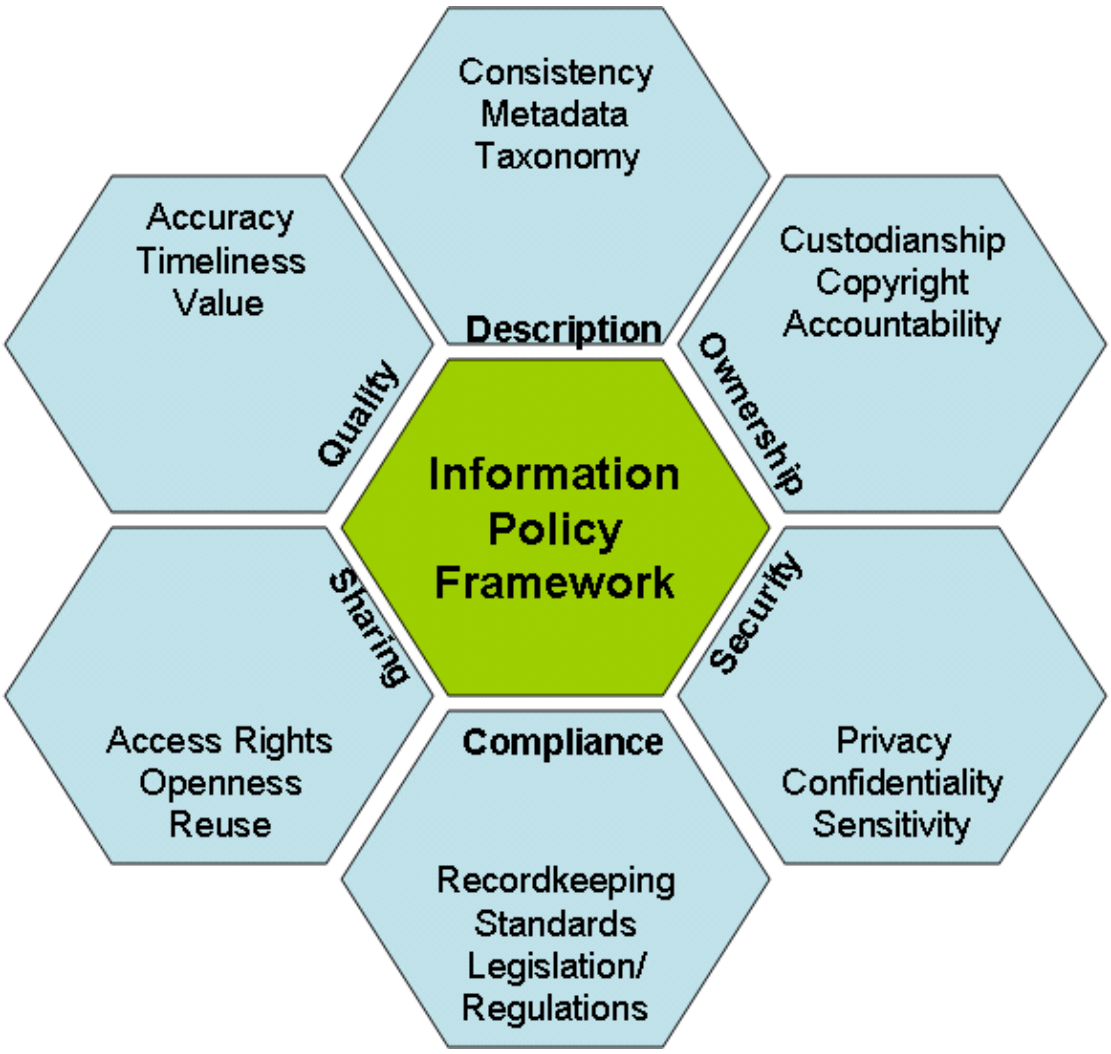
"Records management" refers to the professional practices associated with the management of records through their life cycle, and is particularly relevant to the duties of dedicated registry or records management staff. "Record keeping" is a more general term that also includes the responsibilities of all employees in respect of records creation, capture, storage and use.

Records, like information, have a clear lifecycle. When we assess the records management policies, procedures and practices, just as in information management we are also assessing whether they are able to capture and manage the characteristics of a record through its life cycle from creation, to use, to disposal.

[1] It should be noted that "transaction" is taken to refer to internal and external transactions, operational transactions as well as strategic, planning, reporting, policy and procedural development and project activities.

2. A Framework for Information and Records Management Policy Development

A comprehensive framework for information management policy building will need to cover six main areas, as illustrated in the diagram below.



2.1 Description

Information assets need to be summarised and accurately described if they are to be made visible to other work groups beyond their immediate work context.

Titles, filenames and descriptions need to follow consistent formats and conventions, so that searchers can accurately judge the content of a document from its description. For electronic content, the information describing the documents will be captured in metadata associated with each document, and this will help officers in locating relevant and useful information via the content management system and search engine.

Subject categories also need to be consistently applied, and an organisation wide taxonomy usually forms a subset of the metadata fields to be assigned to a document. If insufficient metadata is assigned, or if it is inconsistently applied, then the assets, although available in the system, will effectively be invisible to users.

For records special metadata is also captured to sufficiently describe their format and processes which need to be applied to them to ensure their integrity is maintained over time should they need to be retained for a long period of time and managed and migrated across systems and software changes.

2.2 Ownership

The widespread and varied use of information across the organisation means that no one group of staff can effectively control and manage all of the organisation's information assets. Responsibility for ensuring proper management of information assets needs to be delegated to managers of operational units throughout the organisation.

The principle of "custodianship" recognises that information is owned by the organisation that creates and uses this information in the course of business, but that there are designated persons throughout the organisation who need to ensure that particular sets of information are adequately and appropriately managed. As such they are the "custodians" of those information sets for which they are accountable. In addition, all officers have a responsibility for the proper creation, use and disposal of information assets.

The presence of a clear policy, identification of delegated responsibilities, and dissemination of good awareness and training on information management policy will all help managers and their staff identify issues of intellectual property and copyright and exercise appropriate controls. With delegated responsibilities the organisation ensures proper accountability for the management of information, and compliance with external regulations and standards.

2.3 Security

All organisations need to protect certain categories of information, whether for commercial reasons or in the public interest. Lack of proper management and control over the creation, transfer, storage and use of documents increases the risk of improper use of information, for which the organisation may be held accountable.

Protection of confidential and sensitive information involves clear definition of custodial duties delegated to managers (see "Ownership" above), and clear, well-communicated guidelines on how to classify the sensitivity of information appropriately, and any special processes governing copying, transfer and use of those classes of information.

Where organisations also collect and use information about members of the public in the course of doing business (such as booking systems, training provision, delivery of medical services), there is also the need to protect information based on privacy grounds, for ethical and legal reasons.

2.4 Compliance

Both commercial and public sector organisations are under statutory obligations to keep their business records in an accessible form for minimum periods of time. Public sector organisations may also have legal requirements to maintain records and also to ensure proper management of those records designated as candidates for national archives.

In the event of litigation, contractual disputes, criminal investigations or official inquiries, the organisation may be obliged by the authorities to produce evidence of the activities and decisions at dispute or under inquiry. It must also be able to produce documentation as evidence of the related business activities and of compliance with government policies and regulations, such as procurement guidelines.

If the organisation holds accreditation according to specific standards such as ISO certification, then it must also be able to manage its information and records to demonstrate continuing adherence to the accreditation standard.

2.5 Sharing

The need to share information assets across the organisation goes to the heart of organisational effectiveness, and underpins any knowledge management effort. An organisation that does not share effectively will always run into issues of inconsistent information being given to stakeholders, partners and customers, poor coordination between business units, lack of timely information to make effective decisions, and unnecessary time and resources being spent on searching for information or duplicating information resources that already exist elsewhere.

The principle of information sharing also complements the principle of custodianship, which states that all information assets created in the course of doing business are the property of the organisation and not the officer or work group that originate them.

The principle of sharing must be balanced against the principle of information security. But even sensitive information should be described and its existence made visible to the rest of the organisation (including who its custodian is) without revealing its sensitive content, so that its potential for reuse by staff with the appropriate clearance can be made viable. If made visible in this way, staff can request access from the information custodian, who can assess the need and either share the document or release a sanitised version of it. The only class of documents that might not warrant such visibility would be top secret documents.

Hence in publishing information assets for reuse in the rest of the organisation, it is important that custodians decide the appropriate level of access based on their sensitivity, balanced with the desire to make information assets visible. The principle of access control should always be “restrict access only if there is a clear criterion for doing so” rather than “restrict access unless we know there is a specific need elsewhere” (need to know). Information creators can rarely anticipate the many different ways in which their document might be needed or valued elsewhere in the organisation.

2.6 Quality

There are roughly three kinds of information asset within an organisation:

(a) **business records** that are evidence of decisions and activities (internal and external)
(b) **sharable information assets** created in the course of work but with value elsewhere in the organisation
(c) **working information assets** that have little value beyond the immediate task for workgroup where they were created

Records frequently start their life as working information assets when they are in preliminary draft form and then more to a business record status once released as a finalised draft. On the way they may pass through the status of a shared information asset as well, particularly when preliminary drafts are circulated for comment and exposure.

One of the tasks of information management is to ensure that the types that have value for recordkeeping or effectiveness purposes (a) and (b) are not drowned out by the sheer volume of type (c) documents that have little value beyond their local context.

Type (a) records will have the most effort expended on them, in terms of description, subject categorisation and metadata for controlling access and lifespan. Type (b) sharable information assets will need to have good, consistent descriptions and subject categorisation metadata for enhancing their findability across the organisation. Type (c) requires the least amount of effort, with simple descriptions and sufficient subject categorisation to enable its easy retrieval within its local workgroup.

A three tiered approach like this is designed to enhance timely access to accurate, useful and relevant information whenever and wherever it is required, and to apportion the management effort invested in documents according to their sensitivity and importance.

3. Special Requirements for Records Management

While the Information Policy Framework encompasses both information assets in general and records in particular, records management and record keeping have some special requirements driven by their status as evidence of the organisation's activity.

In the extract below from the ISO 15489 standard on records management, we find that records (wither digital or physical) only retain this evidentiary status so long as four key characteristics are preserved by conscious and consistent management processes:

- Authenticity
- Reliability
- Integrity
- Usability

Essential characteristics of records
(abstracted from ISO 15489-1)

A record should correctly reflect what was communicated or decided and what action was taken. It should be able to support the needs of the business to which it relates and be used for accountability purposes.

As well as content, the record should contain or be persistently linked to or associated with the metadata necessary to document a transaction as follows:

a. *The structure of a record, that is, its format and the relationship between the elements comprising the records should remain intact.*
b. *The business context in which the record was created, received and used should be apparent in the record (including the business process of which the transaction is part, the date and time of the transaction and the participants in the transaction);*
c. *The links between documents, held separately but combining to make up a record should be present*

Records management policies, procedures and practices should lead to authoritative records which have the characteristics below.

Authenticity
An authentic record is one that can be proven
a. *to be what it purports to be*
b. *to have been created or sent by the person purported to have created or sent it, and*
c. *to have been created or sent at the time purported.*

To ensure the authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment.

Reliability
A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities. Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments used with the business to conduct the transaction.

Integrity
The integrity of a record refers to it being complete and unaltered.

It is necessary that a record be protected against unauthorised alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

Usability
A usable record is one that can be located, retrieved and interpreted. It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

4. Conducting a Review of Information and Records Management Practices

In order to identify issues and needs in relation to information and records management, the information policy framework described above will give general guidance on identifying issues for information management.

4.1 Description

- Are there consistent practices in naming, filing and describing documents?
- Is there a standard metadata framework and taxonomy used across the organisation?

4.2 Ownership

- Is there an information custodianship policy in place, so that staff and managers know their responsibilities in relation to documents and records?
- Is there an up to date list of authorised custodians of key information assets and records, for purposes of quality control and accountability for compliance?

4.3 Security

- Are sensitive documents and records classified consistently and is access being controlled accordingly?
- Is there a consistent policy and practice in relation to privacy of personal information?

4.4 Compliance

- Is there a robust records management system in place to satisfy statutory requirements about preservation and availability of business records?
- Is the records management system also protecting against business risk and enabling the organisation to demonstrate compliance with certification and accreditation requirements?

4.5 Sharing

- Is there a consistent practice of making reusable information widely available across the organisation to avoid redundancy and duplication of effort?
- Are such information assets organised and described in a way that makes them visible and easily re-used?

4.6 Quality

- Is it easy to distinguish high value reusable information and business records from lower value, more transient information?
- Do searches in the organisation's repositories return high quality, high relevance results in a majority of cases?

4.7 Records Management

In addition, the following areas will need review to identify more specific records management issues.

- Is there an explicit policy with practical guidelines on the record keeping responsibilities of employees?
- Do the policy and guidelines adequately cover both physical and digital records?

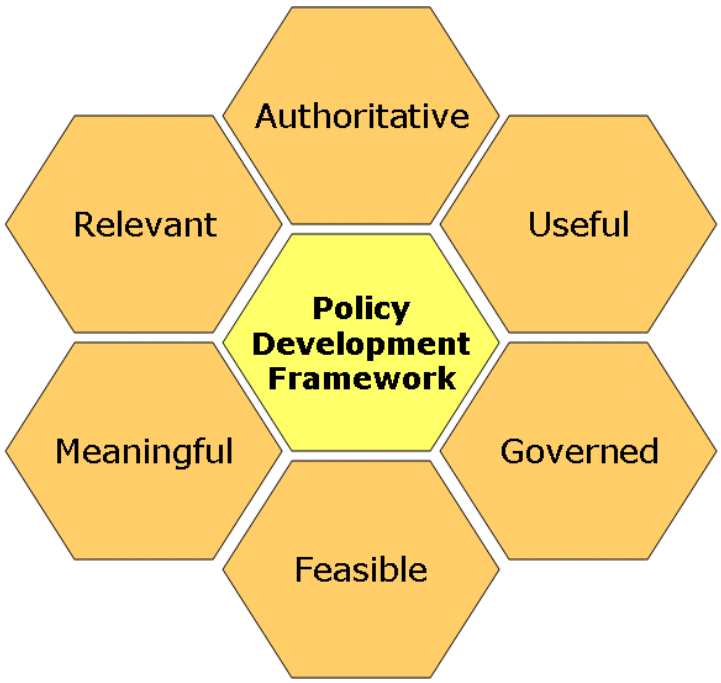
- Do employees have a consistent understanding of these responsibilities and know how to perform what is required?
- Are records being captured and managed so as to preserve their essential characteristics of authenticity, reliability, integrity and usability and to maintain their content, context and structure?
- Does the taxonomy/classification scheme reflect the nature of the business activities, so that they provide easy and timely evidence of those business activities and does it provide the framework against which records are assessed for retention and disposal purposes?
- Is the storage and management of records consistent with their preservation and accessibility needs throughout their lifecycle?
- Is the full lifecycle of the record being managed consistently, and are records being destroyed or archived in accordance with statutory and business requirements?
- Are document management systems capturing all of the necessary administrative metadata necessary for maintaining the essential characteristics of digital records (authenticity, reliability, integrity and usability), and are the workflow processes consistent with the records management policy?
- Is there a business continuity plan and process in place to ensure the organisation's vital records will be preserved in the event of a major disaster?[2]

[2] Vital records are those records that are necessary to enable an organisation to reconstitute its business and continue to meet its obligations

5. Developing an Information and Records Management Policy

5.1 Principles for Policy Development

Information and Records Management Policy, like any other kind of policy, must fulfil the principles of good policy. A generic framework of principles for building sound policies is given below.



Authoritative
Policies should be compliant with existing regulations and statutory requirements, and enable compliance with them. They should also be guided by the vision, values, strategies and objectives of the organisation that they belong to.

Useful
Policies should actively enable the organisation to achieve its objectives and perform its operations in an effective manner. They should give sufficient guidance to be able to generate procedures and guidelines for practical implementation. They require continuous feedback on how well they perform this role.

Governed
Policies should have a clear accountability to the leadership of the organisation, and they should be developed in consultation with all key stakeholders involved in policy implementation and use.

Feasible
Policies should be pragmatic and achievable, representing a “better practice” goal rather than an unachievable ideal state. This is done by an assessment of current state and comparison with “better practices” elsewhere.

Meaningful
The purpose, value and importance of the policy should be clearly understood by all employees whose actions are bound by it. Any policy needs a communication, education and awareness plan.

Relevant
The policy should be appropriate to current conditions and objectives, and therefore needs to evolve as the internal and external environment around it changes. The governance structure should therefore provide for regular review.

5.2 Steps in Policy Development

A generic process for policy development would usually contain the following steps:

- **Analyse needs** – may be generated by a formal review, new legislation, change in strategy, issues with current policy
- **Identify and charter governance structure and stakeholders** – should be in line with normal governance structures of organisation, will cover policy development, authorisation, implementation, ongoing support and regular review
- **Define scope and objectives** – will consider purpose of policy and desired outcomes, existing policies and practices, good practice examples from elsewhere, key stakeholders and end users, impact on working practice, change management
- **Draft policy** – follow a consistent structure / policy template, use simple, direct language, include definitions of key terminology, reference related policies
- **Consult** – with key stakeholders, business owners, staff directly affected by the policy, seeking feedback on feasibility, clarity, usefulness, conflict with other policies and procedures
- **Publish policy** – seek authorisation from the appropriate body defined in the governance structure, communicate to affected staff, support with training and awareness programme
- **Review** – conduct formal review after one business cycle, collect feedback, amend and re-publish as necessary
- **Monitor and Manage** – establish mechanism to monitor compliance with policy, offer additional support where required, or revise policy accordingly, conduct regular (annual) reviews

5.3 Structure and Content of a Policy Document

A generic structure for a policy document would normally contain the following elements:

- Statement of purpose
- Scope of policy, which areas, functions or situations it covers
- Definitions for key terms
- Policy statement of the key principles expressed by the policy
- Responsibilities of officers for carrying out the functions of the policy
- Delegation of authority required to take necessary action under the policy
- Guidelines for implementation
- Implementation and review mechanism

- Communication and support mechanism
- References to related policies
- Authorities, giving any superordinate mandates, policies or regulations under which this policy falls

5.4 Information and Records Management Policy

Some policy areas are very broad in scope, and cut across numerous functions and roles, and information and records management is an example of this. In many instances, a review of the existing policy and practice environment will reveal a number of pre-existing policies affecting some areas of information and records management and not others. They may or may not be consistent with each other, and they may be at varying stages of acceptance and relevance.

In this case, a single policy document will usually not satisfy the organisation's needs, and it will need to develop an integrated framework of information and records management policies and sub-policies. This is illustrated in the table below, which shows a generic framework to cover typical examples of information and records management needs.

Legislation, Statutes, higher level Policies	Knowledge & Information Management Policy Statement					
	ICT	**Description**	**Ownership**	**Compliance**	**Sharing**	**Quality**
	ICT Security & Sub Policies: •Desk top systems •Electronic Mail •Electronic Public Services •Internet / Intranet •Use of Authorised Software •VPN •Mobile Computing •ICT Procurement	**Sub policies:** •Metadata •Document Control *[Tools – Taxonomy / Metadata Framework / Records Classification]*	**Sub policies:** •Information Custodianship •Information Transfer on Staff Departure •Intellectual Property	**Sub policies:** •Records Management •Email and Messaging Records •Records Discovery •Digital Signatures •Information Security & Privacy *[Tools – Records Retention & Disposal Schedules]*	**Sub policies:** •Library & Information Resources •Sharable Information Assets	**Sub policies:** •Publishing (website & other media)
	All sub-policies underpinned by the need to balance security and sharing					
	All sub-policies provide for all stages of the information life cycle					

At the top, a general over-arching knowledge and information management policy document will state the guiding principles for all sub-policies. Then in each area of our information management framework from section 2 above, the necessary sub-policies will be developed.

In addition to the components of this framework, it may be necessary to add an additional set of ICT-related sub-policies, since ICT has a set of special needs that impact all other policy areas. In this table we have not listed a separate set of sub-policies for information security, on the assumption that this will be provided for as an integral part of all other sub-policies. However, some organisations do develop separate information security sub-policies.

With the exception of ICT procurement, ICT-related policies have a relatively generic content and format. However, other kinds of sub-policy may not be as well-understood, so in the table below, we have given brief outlines of each one.[3]

IM Component	Sub-Policy Title	Purpose
Description	Metadata	Provides consistent description and management information for the organisation's information assets. May also include guidance on data and information quality, including: characteristics of data quality - including integrity, accuracy, consistency, currency and completeness; improving data quality by reviewing, defining, measuring and amending it; addressing management responsibility for maintaining data quality; opportunities and threats represented by implementation and upgrading of computer systems. Alternatively an organisation could develop a separate data quality sub-policy under the category "Quality" below.
Description	Document Control	To give assurance that documents consulted are the correct and up to date versions thus reducing risks of using incorrect documents; to support productivity through the application of templates. Supports security, intellectual property and information quality and auditing.
Ownership	Information Custodianship	To establish an accountability base for the effective management of information. Custodianship responsibilities include ensuring compliance with legal and administrative requirements.
Ownership	Information Transfer on Staff Departure	To ensure proper accountability for the organisation's information assets when a staff member leaves the organisation; includes handover procedures and proper accounting for email and computer records.
Ownership	Intellectual Property	To protect the intellectual property rights vested in the organisation's information. Can include copyright and where it should be asserted, monitored and enforced and managing expiry as well as insuring adherence to copyright owned by others. Alternatively, a separate copyright sub-policy could be developed.
Compliance	Records Management	To establish an accountability base for the management of records throughout their life cycle and to provide a structure to support

[3] This is drawn in part from a publication of the Australian N.S.W. Department of Commerce Government Chief Information Office www.oit.nsw.gov.au

		record keeping awareness raising, training and monitoring. Also provides for the orderly disposal of records to ensure records are retained for only as long as they are required for business, evidential and compliance purposes and that their disposal is managed and accountable.
Compliance	Email and Messaging Records	A separate and special sub-policy to support the records management policy (it could also be embedded in it); needs special attention because of the prolific and fragile nature of these communications many of which are the products of business transaction and decisions and therefore fall within the definition of records.
Compliance	Records Discovery	Provides for an orderly approach to identifying and retrieving all records required by official investigations and Courts and ensures records are not inadvertently destroyed through the normal disposal process and are not inadvertently overlooked with possibly detrimental implications for the organisation.
Compliance	Digital Signatures	Provides guidance on digital document authentication and a structured approach to doing business electronically and the provision of robust evidence when required.
Compliance	Information Security and Privacy	Provides examples of each level of sensitivity and gives clear guidance on preparing and handling classified documents; covers provesses for removal and auditing, copying, storage and disposal, and transmission of such materials. May be merged (or treated separately from) a policy document on privacy and personal information. This will provide direction on personal information and personal data protection including: privacy in the workplace - including information on record-keeping, monitoring and video monitoring; the definition of personal information; the roles carrying responsibility for the management of personal information; considerations when conducting business via the internet. Should possibly be seen more as a guide to explain the policy.
Sharing	Library and Information Resources	Clearly identifies the published information materials created and acquired throughout the organisation to ensure their effective management and accessibility as well as addressing their management when they are both a published item and a record (e.g. a publication by the organisation).

Sharing	Sharable Information Assets	Provides guidance with examples on how to identify information assets that have potential for sharing beyond the immediate workgroup where they are created; identifies the processes involved in making them sharable in terms of document description, use of taxonomy etc.
Quality	Publishing (website and other media)	To provide guidance on the delivery, management, maintenance and quality assurance of the organisation's information and services using the Internet. Links closely to Document Control sub-policy and Library and Information Resources sub-policy.
ICT	ICT Procurement	Provides an understanding of the key information and records management requirements for the successful acquisition of Information and Communications Technologies.

Clearly, in a very immature policy environment, not all of these policies can or should be developed all at once. Hence, in the scoping phase the group mandated with information and records management policy development and governance will need to prioritise and sequence the development of sub-policies subsequent to the development of the main policy document. This prioritisation will be driven by the issues that surfaced in the needs analysis phase, and by pragmatic considerations about the need to improve effectiveness, avoid business risk, and manage change.

Acknowledgements

Policy on the Management of Government Information Treasury Board of Canada http://www.tbs_sct.gc/pubs_pol/ciopubs/TB_GIH/mgih_grdg_e.asp

Guidelines of the New South Wales Department of Commerce Government Chief Information Office http://www.oit.nsw.gov.au

About the authors

Marita Keenan is founder and senior consultant with Alchemy Knowledge Solutions, based in Western Australia. Her career as an independent records and information management consulting spans a period of 20 years, and she is an acknowledged expert in the field.

www.alchemyknsolutions.com

Patrick Lambe is founder and principal consultant of Straits Knowledge, a Singapore-based firm focused on knowledge and information management. Originally trained in library and information management, he subsequently worked in training and development before specialising in knowledge management.

www.straitsknowledge.com
PL/MK/25 June 2006