INFORMATION AND KNOWLEDGE MANAGEMENT FOR CLIMATE CHANGE (IKM4CC)

Guideline 1: Summary of Key Tasks and Recommended Practices

Information and Knowledge Management for Climate Change (IKM4CC)

Guideline 1:

Summary of Key Tasks and Recommended Practices

Griffith University

and

Secretariat of the Pacific Regional Environment Programme (SPREP)

Disclaimer

Griffith University advises that the information contained in this publication comprises general information only. This information is not a substitute for obtaining professional legal and technical advice from your organisation.

Information and Knowledge Management
For Climate Change (IKM4CC)
Guideline 1: Summary of Key Tasks & Recommended Practices

Contents

ABOUT THIS GUIDELINE

This guideline is part of the Information and Knowledge Management for Climate Change (IKM4CC) Guidelines. The purpose of the Guidelines is to help government departments, and other agencies and organisations that deal with issues related to climate change in the Pacific region, to implement good practices for managing information. They have been developed in consultation with representatives from government departments, NGOs and regional organisations based in the Pacific.

While the Guidelines focus on the management of digital data and information and the challenges posed by the electronic information environment, many of the concepts can also be applied to paper-based information.

This guideline provides an overview of the "information lifecycle" and gives summary advice on recommended information and knowledge management practices associated with each step. It directs readers to more detailed information provided as part of the IKM4CC Guidelines, as well as other relevant online resources.

USAGE & DEFINITIONS

Throughout this document the following usage applies:

- ➢ The term *information* is used to include data, information, information assets and knowledge. The terms *data*, *knowledge*, and *information assets* are only used when specific reference is required.
- ➢ The term *organisation* is used to include a variety of organisation types including government departments, intergovernmental organisations, non-government organisations, regional bodies and public and private agencies. Individual types of organisations are used only when specific reference is required.
- ➢ The term *item* is used to refer to an individual information resource. Items can include resources such as books, reports, articles, films, maps, photographs, transcripts, audio or video recordings, and datasets. Items can come in a variety of formats, such as paper, CD, cassette tape, videotape, DVD, and online databases.
- ➢ The term *IKM* is used as shorthand for *information and knowledge management*.

Information management (IM)	The collection, processing, organisation, storage and dissemination of data and information for a specific purpose[1].
Knowledge management (KM)	The leveraging of people, resources, processes and information to achieve a strategic objective[1].
Information and knowledge management (IKM)	The dual activities of information management and knowledge management, which may be undertaken as separate or integrated activities within an organisation.
Data	The representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing[2].
Information	Any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form[2].
Information assets	An identifiable collection of data recognised as having value for the purpose of enabling an agency to perform its business functions[2].
Knowledge	A body of understanding that is constructed by analysing information. Knowledge may be recorded or embedded within people in organisations[2].

WHY INFORMATION AND KNOWLEDGE MANAGEMENT IS IMPORTANT

Information is a resource of critical importance to governments and organisations. It flows through every work process, and impact every decision.

Information is a valuable asset. The goal of IKM is to enable organisations to control, administer, use and share these assets throughout their lifecycle in a secure, efficient and accountable manner that maximises their impact and return on investment.

(i) *Organisations need to make sure that the **right** information is available to the **right** person, in the **right** format and medium, at the **right** time.*

---

[1] Definition from UNISDR 2013, Information and Knowledge Management for Disaster Risk Reduction (IKM4DRR) Framework and Scorecard. Geneva, UNISDR.

[2] Definition from QGCIO 2009, Queensland Government Information Management Policy Framework Definitions. Brisbane, State of Queensland (Department of Public Works).

THE INFORMATION LIFECYCLE

The movement of information through an organisation is often described as a "lifecycle". It can be useful to use the lifecycle model as a way of planning organisational information and knowledge management processes and activities.

The Information Management Lifecycle in **Figure 1** highlights common information management activities.
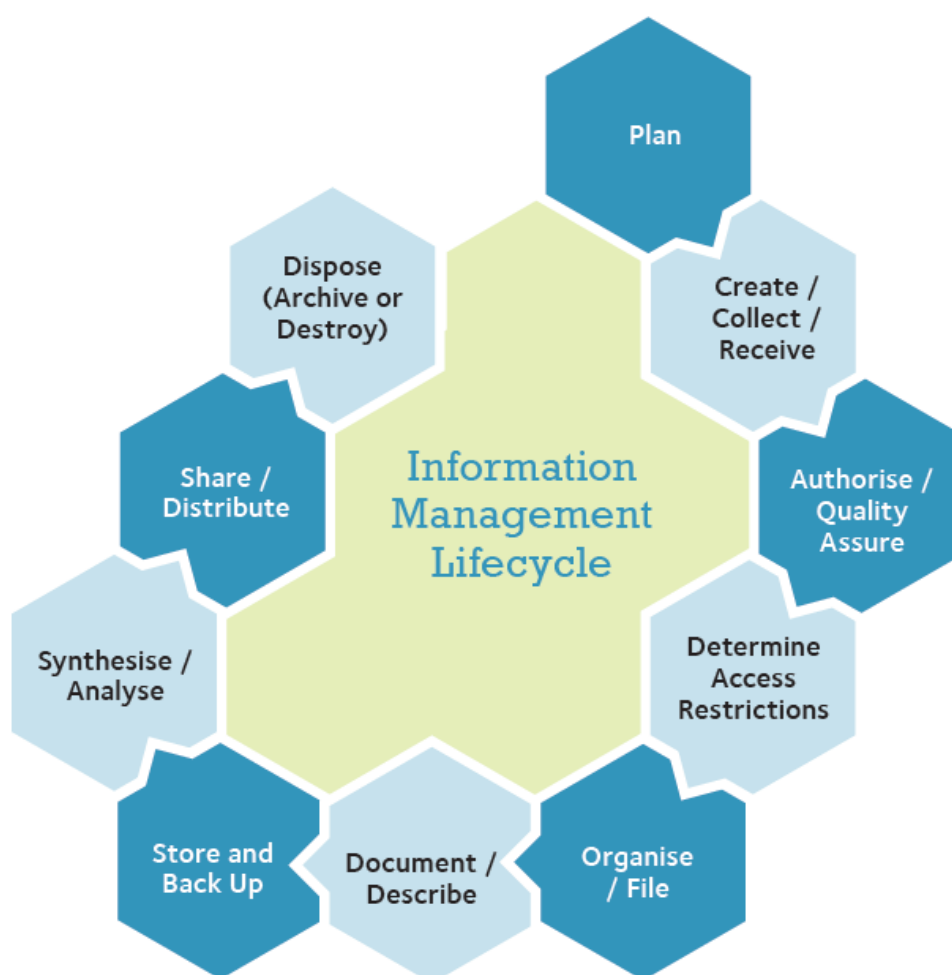

Figure 1. The Information Management Lifecycle

KEY INFORMATION MANAGEMENT ACTIVITIES AND RECOMMENDED PRACTICES

Table 1 lists key issues and recommended practices associated with each step in the information management lifecycle, and provides links to more detailed information provided as part of the IKM4CC Guidelines and/or via other authoritative web-based resources.

Task	Key IM issues	Summary advice	Associated Guidelines Details of relevant guidelines from the Pacific iCLIM **Information & Knowledge Management for Climate Change (IKM4CC) Guidelines**	Useful Links, Examples or Templates
Planning for information management	Guiding strategies and frameworks Organisational readiness to implement new IM initiatives Strategies and systems for managing information Legislative requirements	Develop an information and knowledge management strategic framework which sets out required inputs, governance arrangements, roles and responsibilities, principles, policies, guidelines, and operating procedures. Choose an information management strategy/system that is most suited to your organisation. Assess the maturity of your current information management activities, and the readiness of your organisation to implement and support any new systems or processes. You may like to use or modify an existing assessment tool. Make sure new initiatives have high level support, are demand-driven, standards-based, sustainable, and can be monitored and evaluated. Comply with any legislation, regulations or policies in place in your country or department, e.g. Government Information & Records Management, Information Security Policy, Copyright Legislation, Privacy Legislation, Freedom of Information Policies.	**IKM4CC Guideline 2**: **Preparing for Successful IKM**, includes: • Strategic IM Frameworks • IM readiness and maturity • Overview of strategies and systems for storing and organising information	Model Recordkeeping Policy (PARBICA Guideline 3) http://www.parbica.org /sharing/publications/re cordkeeping-for-good-governance/index.aspx Digital recordkeeping – choose the best strategy (PARBICA Guideline 14) http://www.parbica.org /sharing/publications/re cordkeeping-for-good-governance/index.aspx Digital Recordkeeping Readiness Self-assessment Checklist (PARBICA Guideline 13) http://www.parbica.org /sharing/publications/re cordkeeping-for-good-governance/index.aspx Information Management Maturity Measurement Tool IM3

				(Victorian Government) http://prov.vic.gov.au/government/information-management-maturity-measure-tool-im3
Creating new information	File naming Version control Asset registers Copyright and licensing	Name new files according to a systematic naming convention. Give files titles that reflect what is in the files and are understandable to people using the files. Use a system to keep track of document versions e.g. a version control table within a document. Store master copies securely in a single location and limit 'write' access to them. Consider the use of an asset register to record details of major collections of information or data your organisation has created. If your country has copyright laws, any new information you create will probably be subject to copyright and people may be limited in the use they can make of it. Consider licensing information outputs with a Creative Commons licence, so others can more fully reuse or repurpose them, while still giving your organisation credit.	**IKM4CC Guideline 5**: **Copyright, Legal and Ethical Issues**, includes: • Copyright and licensing issues • Open licensing and Creative Commons Licences	File Names and Folder Structures (UK Data Archive) http://data-archive.ac.uk/create-manage/format/organising-data Version Control and Authenticity (UK Data Archive) http://data-archive.ac.uk/create-manage/format/versions Digital recordkeeping – choose the best strategy (PARBICA Guideline 14) http://www.parbica.org/sharing/publications/recordkeeping-for-good-governance/index.aspx Copyright and Licensing toolkit http://www.oerafrica.org/copyright-and-licensing-toolkit Creative Commons Factsheets http://creativecommon

Sourcing existing information	Information stocktakes Copyright and licensing	A formal stocktake can help you to discover and record what information your organisation or other organisations hold. Make sure you define the purpose and scope of your stocktake before you start. Use an inventory to record details about the information you discover. Before you use or share information created by other organisations, check for any copyright, licensing or other terms-of-use restrictions. You may also discover relevant information by searching other climate change repositories, or using a search engine like Google or Google Scholar.	**IKM4CC Guideline 3: Sourcing Information and Information Sharing**, includes: • Data Stocktake Guidelines and templates • Key Climate Change Repositories • Internet Searching Techniques and Tips **IKM4CC Guideline 5: Copyright, Legal and Ethical Issues**	Example: Stocktake for the Environment Domain Plan 2012 (Statistics NZ) http://www.stats.govt.nz/browse_for_stats/environment/environmental-economic-accounts/environment-domain-plan-stocktake-paper.aspx
Collecting or receiving information	Data sharing agreements/MOUs Asset registers	If you need to collect information regularly from other departments or organisations, consider formalising the arrangement with a data sharing agreement or MOU. Consider the use of an asset register to record details of major collections of information or data that your organisation has collected or received.	**IKM4CC Guideline 3: Sourcing Information and Information Sharing**, includes: • Data Sharing Guidelines • Key components of data sharing agreements	Good Practice Guide to Sharing your Data with Others (Australian National Statistical Service) http://www.nss.gov.au/nss/home.nsf/NSS/E6C05AE57C80D737CA25761D002FD676?opendocument
Transferring information	Secure data transfer Data encryption	Avoid transferring personal or confidential information via email or through a file sharing service like Dropbox. If you must use email to transfer sensitive information, encrypt it first using an industry-standard encryption technology like PGP (Pretty Good Privacy).		Transmitting and Encrypting Data (UK Data Archive) http://data-archive.ac.uk/create-manage/storage/encrypt

		When transferring data using CDs or Flash Drives (USB sticks), make sure the original data is stored and backed up elsewhere.		
Authorising or Approving information	Access control Master copies Authenticity checks	Prevent unauthorised changes to information and data by having a process which outlines who can access and edit documents. Maintain authenticity by keeping a single master file, and control 'write' access to master files. For datasets, consider using infrastructure that offers authenticity checks such as checksums, and provides reports of file corruptions and instances of unauthorised access.		Version Control & Authenticity (UK Data Archive) http://data-archive.ac.uk/create-manage/format/versions
Organising/filing information	File naming Folder naming and structures Use of Business Classification Schemes	Use meaningful file names that uniquely identify files and provide clues to their content and status. Avoid very long file names, and avoid using spaces and special characters. Create a logical folder structure to organise information on network drives so staff can locate information when they need it. Use your organisation's functions and activities as a basis for your folder structure and naming. Consider implementing a business classification scheme based on your organisation's functions and activities. The development of a classification scheme usually requires input from a records management expert.	**IKM4CC Guideline 2: Preparing for Successful IKM**, includes: • Overview of strategies and systems for storing and organising information	File Names and Folder Structures (UK Data Archive) http://data-archive.ac.uk/create-manage/format/organising-data Tips for Managing Shared Folders (PARBICA Guideline 14, Appendix A) http://www.parbica.org/sharing/publications/recordkeeping-for-good-governance/index.aspx Developing and Implementing Record Plans for Core Business

				Functions (PARBICA Guideline 6) http://www.parbica.org /sharing/publications/re cordkeeping-for-good-governance/index.aspx
Documenting / describing information (creating metadata)	Metadata standards and schemas Controlled vocabularies	[Explanatory Note: Metadata is structured information that describes physical or digital items such as documents, images and datasets. It can be compared to the "cataloguing" of materials held in a library.] When creating metadata, try to include all the information a person would need to discover, access, understand and use the item you are describing. Follow national, regional or international standards when creating metadata. This will mean the maximum number of people (and computer systems) will be able to understand and interpret the items you are describing. For example: ➢ use or adapt existing metadata schemas or profiles when setting up repositories, e.g. Dublin Core (widely used, simple metadata standard), Darwin Core (for biodiversity data), ISO 19115/ANZLIC metadata profile (spatial data). ➢ use ISO standards for date formats, languages and geographic information. ➢ use commonly understood terms, preferably from a controlled vocabulary or thesaurus, to describe the subject matter of the item you are describing. Datasets and data collections need extensive metadata if they are to be understood and reused. Describe the "who, what, where, when, why and how" of the data.	**IKM4CC Guideline 4: Metadata**, includes: • Good practice examples of metadata records • Dublin Core metadata element set • List of common ISO standards and thesaurii • PCCP Climate Change Topics controlled vocabulary	Disciplinary metadata (Digital Curation Centre) http://www.dcc.ac.uk/r esources/metadata-standards Vocabularies: Dictionaries, Ontologies, and More https://marinemetadata .org/guides/vocabs Dublin Core (Wikipedia) https://en.wikipedia.org /wiki/Dublin_Core

Securely storing information	Controlling access to information Information backup	Store master copies on your organisation's network drive, on centralised government-approved storage, or on cloud storage services that have been assessed and approved by your organisation. Do not use portable storage media or a non-approved cloud service like Dropbox for master copies. Make regular backups of information to protect against accidental or malicious loss. Always hold at least two copies of information, a working copy and a back-up copy, preferably off site. Use different forms of storage and backup, e.g. network drive and portable hard drive. Be aware that CDs and DVDs are easily damaged by high humidity and changes in temperature.	**IKM4CC Guideline 2: Preparing for Successful IKM**, includes: • Overview of strategies and systems for storing and organising information	Data Security (UK Data Archive) http://data-archive.ac.uk/create-manage/storage/security Data Backup (UK Data Archive) http://data-archive.ac.uk/create-manage/storage/back-up Tips for Managing Shared Folders (PARBICA Guideline 14, Appendix A) http://www.parbica.org/sharing/publications/recordkeeping-for-good-governance/index.aspx
Sharing information	Deciding on suitable accessibility for information Complying with Privacy policies, protecting individuals' identities Ethical and cultural considerations Complying with Copyright laws Using Creative Commons licensing	Share information to the maximum extent possible, through an organisational website or repository (e.g. a government portal) and/or a discipline-specific repository (e.g. Pacific Climate Change Portal, Pacific Disaster Net). Avoid using project websites for long-term storage as they are often not maintained once the project is finished. Consider legal, ethical and cultural issues before sharing information. You will need to limit access to personal information, confidential data (e.g. national defence, endangered species, trade secrets) or culturally sensitive information (e.g. traditional knowledge). Comply with any copyright and licensing restrictions before you share information created by a third party. For example, uploading another organisation's document	**Guideline 5**: **Copyright, Legal and Ethical Issues**, includes: • Privacy, confidentiality and consent • Cultural sensitivities & traditional knowledge • Environmental sensitivities • Levels of access to sensitive information • Copyright restrictions • Open licensing and Creative Commons	Publishing and Sharing Sensitive Data (ANDS) http://ands.org.au/guides/sensitivedata Pacific Regional Framework for the Protection of Traditional Knowledge and Expressions of Culture (SPC, PIFS, UNESCO) http://www.wipo.int/wipolex/en/text.jsp?file_id=184651 AusGOAL Open Access and Licensing

	to maximise reuse of information	to a public website without the copyright owner's permission may be a breach of copyright. Information sharing options include full open access, restricted access, and metadata-only access. For restricted information, you can share basic details about the information resource without making the full resource openly accessible. You can tell people what they need to do to access the full resource (e.g. apply for a password, negotiate access with data owners). Where appropriate, license your organisation's information outputs with Creative Commons licences, so others can more fully reuse or repurpose them, while still giving your organisation credit.	• Website Terms of Use and Disclaimers	Framework http://www.ausgoal.gov.au/ Creative Commons Licences http://creativecommons.org.au/learn/licences/
Reusing information	Complying with copyright laws Seeking permission to reuse information Correctly attributing authors	When using information created by other people or organisations, remember that copyright laws may limit the reuse of original works. Check the terms and conditions of reuse when using copyrighted information, and if necessary seek written permission to reuse. Always attribute (reference or cite) the original author or creator of information you reuse.	**IKM4CC Guideline 5**: **Copyright, Legal and Ethical Issues**	Best Practices for Attribution (Creative Commons) https://wiki.creativecommons.org/wiki/Best_practices_for_attribution
Disposal Overview: archiving or destroying information	'Disposal' of records 'Disposal' schedules Legal requirements	When information reaches the end of its active life, it can be retained permanently as an archive or destroyed. Both of these options are different types of 'disposal'. Check if your organisation has a disposal schedule that tells you what should happen to information at the end of its active life. If not, consider creating a disposal schedule as part of your organisation's IM guidelines or policies. Make sure it conforms to any legislative requirements to retain or archive corporate or government information.		Data Disposal (PARBICA Guidelines 7, 8, 9, 10): http://www.parbica.org/sharing/publications/recordkeeping-for-good-governance/index.aspx

		Check with your National Archives for further information about disposal of government records.		
Disposal A: Long-term preservation or archiving	Planning for technological obsolescence

Avoiding proprietary file formats

Managing storage media

Scanning of paper records | Preservation of digital objects needs to be more proactive than paper preservation. One of the key challenges of preserving digital information is dealing with the fact that computer-based technology (hardware and software) goes out of date. Digital information may have to be migrated to new systems and software over time.

Where possible, avoid archiving information in digital formats that require access to proprietary technologies (e.g. commercial software). Migrate information to open standards to reduce technological dependencies (e.g. formats like CSV, PDF/A, ESRI shapefile, TIFF).

If storing information in proprietary formats, bring records forward as new versions of software are released.

Perform regular backups for disaster recovery purposes.

Carry out routine checks of long-term storage media. Regularly replace media to limit the risk of damage or loss of records (every 2-5 yrs).

Keep storage media in stable, controlled, low-risk, secure environments.

Consider creating digital versions (scanning/digitising) of paper-based information, according to standards and specifications.

Check with your National Archives for further information about long-term preservation of government records. | | Digital Preservation (PARBICA Guideline 18) http://www.parbica.org /sharing/publications/re cordkeeping-for-good-governance/guideline-18.aspx

File Formats (Australian National Data Service) http://ands.org.au/guid es/file-formats

File Formats (UK Data Archive) http://data-archive.ac.uk/create-manage/format/format s

Digitisation (PARBICA) http://www.parbica.org /sharing/resources/digit isation/index.aspx |
| **Disposal B: Destruction** | Destruction process for sensitive or | Be aware that deleting files or reformatting hard drives does not truly erase data files. For complete deletion, | | Data Disposal (UK Data Archive) http://data-archive.ac.uk/create- |

	confidential information	files must be overwritten using special data erasing software.		manage/storage/data-disposal
	Data erasure	Both free and commercial data erasing software utilities are available to securely erase files from hard disks. Data erasure may not work completely on solid state drives or flash based media such as USB sticks.		Compliant destruction of Australian Government Records http://naa.gov.au/records-management/agency/keep-destroy-transfer/destroying-records/index.aspx
	Physical destruction of digital media	The most reliable way to dispose of data is physical destruction. Shredders can be used to destroy paper and CD/DVD disks. Hard disks can be physically destroyed or degaussed (a demagnetising process).		
		Check with your IT department or National Archives for further information on destroying sensitive or confidential information.		

Table 1. Key issues and recommended practices associated with information management