**GUIDE TO INFORMATION MANAGEMENT POLICY TEMPLATE**

**ABOUT THIS POLICY AREA**

An Information Management Policy guides how we organise, store, access and dispose of the various kinds of information gathered in the course of delivering our services and running the organisation. This is an important aspect of ensuring privacy and confidentiality for service users and staff, but it is also vital to business continuity and accountability. In the event of any claim against the organisation (legal or otherwise), good information management enables us to track and demonstrate our decision-making process. Finally, it is integral to quality assurance and the control of documents, such as policies and procedures, which guide our organisation and the decisions we make.

**Policy checklist**

The following checklist will help you check that an existing policy covers this area adequately.

The policy should:

* say how the organisation will communicate information within the organisation, to service users and other stakeholders
* say how the organisation maintains and controls up to date Policies and Procedures which are accessible to staff and management
* say how service user information is securely stored, and access controlled to protect privacy and confidentiality. (You may also refer to other policies such as Privacy, Confidentiality and Access to Confidential Information)
* say how the organisation maintains up to date information regarding staff and securely stores that information
* say how you archive information securely for the relevant timeframes, and how you dispose of information following those timeframes
* describe how you securely store and regularly back up electronic records, including service delivery information, and maintain computer systems.
* set down rules or conditions for staff using computers, email, internet and/or social media, or refer to a separate policy or guidelines which detail these.
* contain clear procedures and actions
* indicate the timing of any actions
* show when it was approved
* show when it was last reviewed.

**COMPLETING YOUR INFORMATION MANAGEMENT POLICY**

**Using the policy template**

The template provides some example statements. You can adapt these statements and include them in your policy or write your own statements to better suit the operations and services of your organisation.

The policy templates include **red text** prompts to insert information that is specific to your organisation.

**Guidelines for each section of your policy**

***1. Purpose***

When identifying the purpose of the policy, consider how it might apply to your particular services, organisation assets and your organisation’s service agreement. This policy supports the commitment to privacy and confidentiality, but also provides the basis of quality assurance for all aspects of your organisation. Do you need to make specific statements to ensure you are inclusive of particular groups, such as Aboriginal and Torres Strait Islander peoples, Australian South Sea Islanders, people from culturally and linguistically diverse backgrounds and people with a disability?

***2. Scope***

To determine the scope of the policy, consider the following questions:

• Does this policy apply to all your organisation’s services and activities or just to those related to the service agreement? Generally, information management applies to all aspects of an organisation.

• If you are including aspects of information management other than those related to service delivery and service goals, what are these, and will different procedures apply to them?

***3. Policy statement***

If you are adopting the policy statement in the template, consider whether there are any additional commitments your organisation wants to make.

In identifying the actions your organisation will take to implement this policy, you should include the following:

* Communicate effectively with staff, service users and stakeholders through meetings, reporting processes, training, newsletters, email and letters
	+ Maintain up to date Policies and Procedures which are accessible to staff and management
	+ Collect service user information in accordance with the Privacy Act and securely store that information
	+ Maintain up to date information regarding staff and securely store that information
	+ Archive information securely for the relevant timeframes, then dispose of information/documentation in an appropriate manner
	+ Securely store and regularly back up electronic records, including service delivery information and maintain the computer systems
* Maintain responsible controls over staff and volunteer use of the internet, email and social media to both access information and to distribute information ( or have a separate policy which deals with this).
	+ Regularly audit and review information management systems and processes to identify improvements on an ongoing basis.

***4. Procedures***

The procedures describe how your organisation achieves the aims and goals you have outlined in your purpose, scope and policy statement.

*4.1 Communication Strategies*

Underpinning the management of information are the following internal and external communication strategies:

* Regular and structured meetings that involve all staff
* Regular reporting to Management Committee
* Training for staff in relevant policies, procedures and work practices
* Involvement of staff and service users in the continuous improvement process
* Involvement of staff, service users and stakeholders in the planning process
* Emails and memos to staff as required
* Letters and notices to service users as required.
* Provision of information (brochures or handbook, etc) to service users
* Reporting/participation in service networks or collaborative groups
* Website, social media, email networks
* Advertising in print media, television, radio.

List those that apply to your organisation. Note links to other policies or plans (eg: Marketing Plan) where relevant.

*4.2 Policies and Procedures*

Organisation Policies and Procedures include several components. In this section, detail the processes which govern the control of these important organisation documents. For example:

1. The Policies and Procedures Manual, which is generally maintained in hard copy and electronically
	1. Where is the hard copy (master) kept and who is responsible for keeping it up to date? Other staff can access the Manual, but must not remove or alter contents. Additional hard copies may be made, but this is a controlled document, so each copy must be numbered and its location noted. This is to enable management of updates and ensure all copies are current. For example, you may provide a full or part manual to board members. If any of these policies are updated, replaced or removed, these changes should be made or communicated to those board members.
	2. A master electronic copy should also be maintained on the computer system in a folder named “Master Policies and Procedures” or similar. This is a read only file, with only selected staff having editing rights. This ensures that these “master”

documents are correct and cannot be altered unintentionally.

1. Forms – organisations develop a range of forms for many purposes, to gather or record information. These documents should be consistent with current policies. Staff should know what forms exist, when to use them and for what purpose. Forms are often updated, and, like policies, need to be clearly identified to ensure they are the current version. The following suggested process for locating forms helps to control these documents:
	1. Copies of Forms relating to sections of the Policies and Procedures Manual are stored at the back of that section in the hard copy of the Manual. Individual Policies list related forms and documents at the end of the document.
	2. A master electronic copy is also maintained in organisation’s computer system in a separate folder named “Forms – Master Copies”

The **staff position/s**, is responsible for ensuring all Policy and Procedures information is up to date – hard copies and electronic. The involvement of all staff is encouraged to ensure policies and procedures reflect practice and to foster ownership and familiarity with the material, however, only the **staff position/s** is authorised to amend or create policy files.

All staff can access the Policies and Procedures either through their own (or shared) computer terminal. If staff require a paper copy of procedures these can be requested from their supervisor but once printed are uncontrolled and should only be used as an immediate reference.

*4.2.1 Updating Policies and Procedures and Forms*

Identify under which circumstances the need to update policies and procedures or forms may arise, such as:

* Changes in legislation or regulations
* Changes in funding or funding guidelines and requirements
* Feedback
* Management decisions and changes in organisation size, structure, services delivered
* Adverse Event Reports
* Audits and Reviews.

Clearly outline the process for updating the policies and procedures, and forms. Your organisation may have developed an agreed process. To some extent, the complexity of the process may vary with the size and complexity of an organisation. The following suggestions ensure that current versions can be identified from drafts, and that changes to policies can easily be tracked. The Coordinator position has been used, but your organisation may identify another position responsible for this work.

1. When the need for changes is identified these are discussed with the Coordinator(or other staff position).
2. The Coordinator develops draft changes with the assistance other staff or delegates this task to other staff.
3. Draft changes are reviewed by the Coordinator who also reports the changes for Management Committee/board approval.
4. During this process, amended documents are clearly filenamed and watermarked “Draft” and stored in the *Draft Policies and Procedures* sub folder on the computer system.
5. When changes have been approved, the Administration Officer is advised to update the Policies and Procedures Manual.
6. The Policy and Procedures Manual is updated including forms and the table of contents. Old versions are watermarked “Obsolete” and archived in the *Obsolete Policies and Procedures* sub folder.
7. Note that any new form is referenced in the Policies and Procedures Manual – Index and related policies. New Policies are numbered according to the relevant section in the Manual, using the next available number. Eg: Current policies in Section 4 are 4.1, 4.2, 4.3, next new policy will be 4.4. If a new policy replaces an existing one (even if it is named differently) it can assume the number from the previous policy.
8. Staff are advised of changes to the Policies and Procedures either through a staff meeting, an email, a memo or a training session. Service users are advised, as appropriate and necessary, through staff, newsletters, letters or flyers.
9. Major changes are recorded as an improvement in the *Continuous Improvement Plan*
10. Major changes are reviewed after an appropriate time to ensure they have achieved the required outcome.
11. The Coordinator reviews the minutes of all management committee/board meetings for decisions that need to be reflected in changes to policies and procedures or forms.
12. Policies and Procedures, including Forms, are reviewed over a three year period. Review dates are noted on each Policy, and a calendar of these dates is also filed in the Master Policies and Procedures folder on the computer system.

*Process for making changes to policies, procedures and forms:*

Whenever changes are to be made to the policies and procedures manual or a form the following procedure applies:

* Before making changes copy the existing file into the *Obsolete* folder
* Watermark the document ‘Obsolete’
* Add ‘Obsolete’ and ‘today’s date’ to the end of the file name – e.g. Corporate Governance Obsolete 03032011
* The original document remains in the *Master Policies and Procedures* sub folder until the amended policy has been approved. The original document can then be finally amended or deleted and replaced with the new policy.
* During the Draft stage, a copy of the original document (or a new document, if a new policy) is made in the *Draft Policies and Procedures* sub Folder. This version is watermarked “Draft” and saved as Policy Name. Version no. Draft. Date. Eg: 4.1 Information Management. V 1.1 Draft 03032013
* The same process applies for the amendment or creation of new Forms, except that they are saved in the respective Forms sub folders.
* *Version Numbering*: the number to the left of the point indicates the number of final, approved or master versions of that Policy; the number to the left of the point indicates the number of drafts for that version. Eg: a new policy may have versions 0.1, 0.2, etc until it is finalised and approved, at which point it becomes 1.0. When that policy is reviewed and amended, drafts will be numbered 1.1, 1.2, etc, until it is finalised and approved, at which point it becomes Version 2.0, and so on.

Obsolete policies and procedures and forms are destroyed as per the timelines listed under 4.7

*File Naming for Policies and Procedures and Forms*

It is useful to have standard filenaming of these documents to facilitate location and searching on the computer system. For example:

* All Policies and Procedures must be saved as:

No. Policy Name. Version No. Status. Date. Eg: 4.1 Information Management V 1.2 Final 10032013.

* The Footer on the Policy should be the same and also include Page x (number) of y (total number).

*4.3 Service User Information*

Storage and access to this information should be detailed in your Client Records policy, so it is adequate to just make reference to these for this section.

The Access to Confidential Information, Privacy and Confidentiality Policies detail procedures for protecting the privacy of information and providing access for service users to their personal files.

*4.4 Staff and Volunteer Information*

Identify where staff and volunteer files are kept (should be a secure/locked location) and who has authority to access and/or make these available to staff members.

Detail the process for requesting access by a staff member, and any conditions (eg: cannot be removed from office, copies only provided if being removed, access noted in the file.) It is important to protect these files from alteration or unauthorised access by third parties. You may have a contents list inside the file cover, which also notes any file movements.

Are any staff file contents also held electronically? If so, how are they protected?

*4.5 Minutes of Meetings*

Minutes of meetings are maintained on the computer system in **name of folder/s.**

Hard copies of board/committee minutes should be maintained and signed by the person chairing the meeting. These are required as part of incorporation reporting, and are an important record of decisions made. They may also be required as evidence of authority, such as when setting up bank accounts.

You may list the types of minutes which you organisation stores. Even staff meeting minutes may be important in the event of a staff or service user complaint.

You may wish to identify some basic requirements of meeting minutes, eg: date, time, location, those present, clearly identify decisions made and actions to be taken and by whom, etc.

*4.6 Other Administrative Documents*

* Where is all other administrative information including funding information, financial information and general filing kept?
* You should include any provisions for security of this information.
* You should also have clear systems for processing incoming and outgoing information. Organisations vary in relation to the amount of information processed and stored electronically. For example, correspondence originals may be entered into a register and then filed, or may be scanned and saved and the originals shredded. Hard copies would normally be retained of signed contracts and legal documents. These procedures should be documented.

*4.7 Archiving*

A position should be identified that is responsible for archive management. Identify where Archived files are stored. How are the archives organised? For example:

Archives are sorted by year and grouped as follows:

* Service user records
* Staff records
* Administrative records including financial records
* Policies and Procedures.

All archived information should be entered in an *Archives Index*. The index records the date of archiving, the file contents, the archive box name and number and the file number and date of destruction.

*Timelines for Retention of Documents*

Identify how long archives are stored for. Some common examples are:

|  |  |
| --- | --- |
| Employment applications unsuccessful | 6 months |
| Staff records | 7 years after the staff person ceases employment |
| Service user records | This will vary according to your service agreement; records for children in care will generally need to be retained until they turn 18, Aboriginal and Torres Strait Islander client files are generally retained indefinitely. |
| Financial records | 7 years |
| General administrative records | 7 years |
| Policies and procedures | One year  |

Identify how you dispose of information following these periods. You may need to check your service agreement for any particular requirements.

*4.8 Electronic Data*

* What kinds of data is stored on the computer system?
* Who has authority to add new data/subject folders to the system.
* If staff require a new data/subject folder to be created, what is the process? You may have different “levels” in your system eg: staff can create folders in their own drives, but not on shared drives.
* Who has authority and what restrictions/processes apply regarding installation of new programs or software?
* What arrangements do you have to back up data and who is responsible? This may be done internally, or by an external IT company. Ideally, there should be a copy of back up data held off-site (or cloud) to protect against loss in the event of disaster, fire or break-in, for instance. Detail any processes for your organisation.
* What programs and processes are in place to protect against viruses?
* Does your organisation have multiple sites and/or remote access? What arrangements are in place to manage this?
* Inappropriate use of computers and the internet can expose services to a range of risks, so it is advisable to provide all users with clearly documented procedures and rules or guidelines. Staff who require access to the computer system may be required to sign a staff computer use and internet agreement form.
* Organisations should have systems in place to protect the security of data held on the computer system, such as all staff who need access to the computer system being assigned a secure password to log on. Who is delegated to administer this process? Computer systems may also be set up so that staff have appropriate levels of access to files. This may include ability to create and edit certain files, read only access to some files and no access to certain confidential files. Who determines levels of access?
* Staff will also be conscious to save files in the appropriate format (eg:Read Only) and if necessary identify staff who should have access.

*4.8.1 Emails*

* Emails can form a significant part of an organisation’s information system, often replacing hard copy correspondence, records of conversations, requests and actions.
* Identify any rules pertaining to emails, such as personal email usage, circumstances where email should not be used (such as most client communication, personal confidential documents, etc).Which emails should be saved and where? For example contracts or formal letters may be received by email and need to be saved to a particular location.
* Email data can cause problems to computer system speed and functioning if traffic is heavy. Are there any rules or procedures about limiting inbox sizes? Are there any rules or protocols about sending receiving emails in terms of file size, or preferable times when large or mass emails are sent? Any protocols regarding inclusion of email addresses in group emails, signature blocks and indemnity/disclaimer footers?

*4.9 Maintaining Computer system and electronic data systems*

* Who provides technical support (internally and/or externally) and how can this be accessed?
* If support is provided by an external company, what does this cover, and who is authorised to access this support/service?

***5. Other related policies and documents***

List the other policies related to the Information Management policy. The policy should be linked to the following policies:

* Access to Confidential Information
* Client Records
* Privacy
* Confidentiality
* Internet Use ( if you have a separate policy)
* Performance monitoring and reporting

Other documents:

* Policy and Procedures Template
* Staff and Volunteer Confidentiality Agreement
* Internet Usage Conditions Acknowledgement for staff and volunteers
* Archive Index/Register
* All policies and procedures, forms and contracts (no need to itemise)

***6. Review processes***

Consider how often the policy should be reviewed and the process for doing this:

• **frequency of review:** Most policies benefit from an annual review. The experience of implementing the policy is used to decide which changes are necessary. Consider reviewing your information management policy as part of an annual review of your organisation’s governance-related policies or, if your organisation is small, perhaps over a three-year period. Critical incidents may prompt you to review the policy ahead of schedule.

• **responsibility for the review:** In most organisations, the board or management committee would be responsible for reviewing this policy in conjunction with senior staff.

• **process for the review:** Decide which particular staff, volunteers, external people and organisations will provide input to the policy review,

• **decision-making process:** Who will review draft changes to the policy and approve changes? What will be the timeframe for the review process?

• **documentation and communication:** What records of the policy review process are needed? How will changes to the policy be communicated to staff implementing the policy? In a small organisation, this may be as simple as noting the changes at a staff meeting. In a larger organisation, an email memo may be needed.

• **key questions for the review:** Is the policy being implemented? Are procedures being followed? Is the policy clear? What has changed that may prompt a change to the policy Have particular stakeholders had difficulty with any aspect of the policy? Can their concerns be resolved? How does the policy compare with that of similar organisations?