**Normal administrative practice (NAP) policy – template**

This policy template outlines the key aspects and components to include in a normal administrative practice (NAP) policy.

As outlined below, you will need to consider your risks and business environment when developing your policy.

The suggested content and text in square brackets can be changed to suit the particular needs of your agency.

**Components**

**Title**

*Insert title*

**Date and version number**

*Insert date and version number, or include a table of document changes.*

**Purpose**

*Explain why a NAP policy is needed and the benefits of good practice. For example:*

The purpose of this policy is to clarify responsibilities and to advise staff and contractors which type of information can be routinely destroyed in the normal course of business.

The benefits of compliance with this policy include more efficient work practices and the management of retained information as a business asset.

This policy is written within the context of [the agency's] information governance framework [or other key document] which is located at XXXX.

**Policy statement**

*Provide a brief policy statement of the agency’s commitment to managing its business information efficiently, as business assets, using NAP. If applicable, mention briefly factors influencing the use of NAP within the agency. For example:*

Normal administrative practice — also known as NAP — is used to delete certain types of low-value and short-term information where there is a low level of risk.

NAP is applied by everyone who works with government information. Information might be destroyed inappropriately if staff and contractors don’t understand what they can and can’t destroy as a normal administrative practice.

**Scope**

*Specify who and what aspects of the agency’s business the NAP policy covers, including the business applications and systems such as websites, email and business systems. For example:*

This policy applies to all [agency] staff and contractors.

It applies to business information in all formats including documents, email, voice messages, audio-visual materials and data in business systems (eg. websites, social media applications, databases).

Individual staff, contractors and outsourced providers are responsible for deciding what low risk business information can be destroyed as a NAP and when it can be destroyed (ie. when the information is no longer needed).

**Legislation and other regulatory requirements**

*Your information governance framework and other key documents cover the legal, regulatory and business context within which your agency operates.*

You might specifically mention requirements that more directly affect staff, for example specific legislative requirements for destroying or keeping particular business information. You may wish to add that:

Use of a normal administrative practice for destroying information is permitted under the Archives Act 1983 section 24(2)(c).

**Risk assessment**

*Your policy should include a statement about the risk assessment that was carried out and highlight residual risks and responsibilities. For example:*

This policy is based on assessment of the risks involved in the use of NAP in [agency].

However, individual staff members are responsible for deciding which low-risk business information can be routinely destroyed using a NAP once the information is no longer needed.

This policy is supported by complementary policies and additional guidelines and procedures which are located at [insert reference].

The [agency information management unit] can provide specific advice for business areas or functions.

The risk categories for business information are as follows:

**Information about destroying business information for all staff and contractors**

*Describe the policy in more detail, explaining when and how it applies. Any procedures or fact sheets explaining the use of NAP should link from here.*

*Explain that NAP differs from agency to agency – what they may have been able to destroy at a previous agency may not apply here.*

Business information considered for destruction using a NAP can be arranged into four broad groups, depending on the level of risk. These apply to information in all formats.

Ideally you should include some examples of specific types of business information in your agency.

You can add or remove from the list of options below:

**Delete with confidence**

* Non-business information such as personal unofficial emails, spam, unsolicited junk mail like ‘hot offers’, non-business related material
* Documents or other information that has already been saved into [the agency’s] approved information management system
* Externally published material and unofficial information
* Reference copies (not master copies) of newsletters, procedures, guidelines, circulars, manuals, policies.

**Delete with care**

* Low-risk emails such as system reminders and alerts, discussion lists and RSS feeds, duplicate emails kept for reference purposes, parts of an email thread where the full thread is saved into [the agency’s] information management system, ‘for your information’ communications, email bounce backs
* Invitations, diaries and calendars (with the exception of SES)
* Duplicates of [Agency] publications and promotional material. Note: the business area responsible for the publication has responsibilities to keep master copies. Contact the [Agency information management unit]. Check before deleting
* Drafts, rough or routine calculations and working papers
* Business information held in shared work spaces such as shared drives and business systems
* Some ICT information such as backup tapes created for business continuity and recovery, some computer logs, some data clean-ups
* Documents prepared with the involvement of senior staff; these are often important and may not be appropriate for destruction using NAP.

**Do not delete**

Valuable business information that is required:

* for accountability purposes and to support decision making
* to protect the rights and entitlements of individuals, groups or the government
* to meet community expectations

**Information about NAP for information management or other specialist staff**

*It’s important for specialist staff to understand when NAP can be applied. For example, you might want to provide specific advice about the use of NAP or its limitations in relation to backup tapes for some business systems, or when records authorities need to be applied.*

*In this section include additional information for any target groups such as specialist information management or IT staff. For example:*

* NAP cannot be used as part of a sentencing activity
* Information that is covered by a records authority can only be destroyed in accordance with the records authority
* NAP cannot be used to destroy [information in xyz business system].

**NAP exceptions**

NAP must not be used to destroy information where any of the following apply:

* Information that is likely to be required as evidence in current or future legal proceedings
* Information that is required to be kept by law (including by a records authority or disposal freeze)
* Information that is required to be kept under an agency policy, procedure or guideline
* Information that is a draft of a Cabinet or ministerial submission
* Information that is a draft of an agreement or other legal document
* Information that is needed to document a significant issue
* Information that is needed to clarify, support or give context to an existing record
* Information that is needed to show how a decision was made
* Information that is needed to show when or where an event happened
* Information that is needed because it indicates who made the decision or gave the advice
* Information that is needed because it contains information on the rights, privileges or obligations of government, organisations or private individuals
* Information that is a draft or working paper that contains decisions, reasons, actions and/or significant or substantial information where this information is not contained in later documents or the document remains not finished.

If you are unsure about any of these contact the [Agency information management unit] before destroying the information.

**Roles and responsibilities**

*Define the roles and responsibilities of all agency employees and contractors to ensure that business information is appropriately destroyed using NAP. This may include:*

All [Agency] staff, contractors and outsourced providers [delete any not applicable]:

* are familiar with the [Agency] NAP policy
* understand their personal obligations and responsibilities when using NAP
* are responsible for identifying information connected with their business activities that may be eligible for destruction as NAP
* destroy information that clearly meets the NAP policy criteria when it is no longer required
* ensure that where information is identified for destruction under NAP, the method of destruction employed is appropriate to the security classification of the content
* seek guidance from [Agency information management unit] if there is any uncertainty over the use of NAP.

The [Chief Information Governance Officer] and/or [Information Governance Committee] of [the Agency]:

* authorises the [Agency] Normal Administrative Practice policy
* ensures that the NAP policy is adequate to the needs of the [Agency] and is consistent with the [Agency] Information Management Policy and the [Agency] Information Governance Framework
* provides sufficient support and resources for ensuring the successful implementation of the policy and guidance
* promotes compliance with the policy
* ensures that adequate guidance is produced to support [Agency] staff, contractors and outsourced providers [delete any not applicable] in understanding and implementing the NAP policy
* reviews and revises the NAP policy as required to ensure it remains appropriate.

All managers and supervisors of [Agency] staff and contractors:

* promote understanding and use of the [Agency] NAP policy to staff and contractors under their supervision
* incorporate NAP policy directives into their business unit work procedures, where appropriate
* liaise with the [Agency information management unit] in relation to using the NAP Policy or any barriers to its use and advise the unit of any changes in the business environment which would impact on information management requirements, such as new areas of business that need to be covered by a records authority
* encourage and support staff and contractors in the compliant destruction of information that is eligible for destruction under the NAP policy once they are no longer required for business purposes
* monitor staff and contractors under their supervision to ensure that they understand and comply with the NAP policy and guidance.

All contract managers:

* are responsible for the insertion of information management provisions (including NAP) into agency contracts with outsourced providers and contractors
* regularly monitor outsourced service providers and contractors with whom they have a contract to ensure that they understand and comply with the NAP policy and guidance.

All ICT staff:

* assist in incorporating NAP policy into the design and development of the [Agency’s] information management systems, including business and IT systems
* ensure that any actions, such as removing data from systems, storage or folders, are undertaken in accordance with this and other relevant policies.

The [National Information Manager and/or other staff with responsibility for [Agency] business or information management systems and services]:

* promulgate the [Agency] NAP policy and provide guidance to all [Agency] staff, contractors and outsourced providers [delete any not applicable]
* provide appropriate training and advice to all staff on the appropriate implementation of the NAP policy, including induction sessions for new staff;
* encourages the incorporation of NAP policy directives into business unit work procedures
* ensures that the NAP policy is incorporated into the design and development of the [Agency’s] information management systems, including business and IT systems
* monitors compliance with the NAP policy.

**Communication and training**

*Include a statement affirming that the policy will be communicated to staff and that training and other support will be provided on aspects of the NAP policy.*

**Monitoring and review**

*Make a commitment to review the policy and monitor compliance. For example:*

The [senior manager responsible for information management] will review this policy every five years, or earlier if required.

[Agency] information management staff (with the support of workplace supervisors) will monitor the compliance with the NAP policy. Levels of compliance will be reported [at least annually] to the [Information Governance Committee].

Supervisors and managers will monitor their respective staff and contractors to ensure the NAP policy is implemented correctly.

Contract managers will monitor compliance of contractors and outsourced service providers with the NAP Policy.

**Resources**

*If necessary, supply a list of resources that provide additional information. This should include contact details of relevant staff within the agency as well as useful reference material.*

*Add information about where staff can get help making decisions about NAP.*

**Senior management endorsement**

*Provide evidence that the [Chief Information Governance Officer (CIGO)] has endorsed the policy.*

*This may be done in a brief paragraph signed by the [CIGO] recognizing the important place of business information in the agency and directing staff to comply with the requirements of the policy.*