

Managing digital records: 1

Contents

Purpose of this guidance	1
1. Make digital recordkeeping achievable for your organisation	1
1.1 Share responsibility for managing digital records	2
1.2 Limit the number of file formats used in your organisation	2
1.3 Use open formats.....	2
1.4 Use templates	3
1.5 Apply standard creation rules	3
1.6 Destroy digital records when appropriate.....	7
1.7 Implement a 'technology watch'	8
1.8 Plan for the costs of digital preservation	9
1.9 Use removable media only when you have to	10

Purpose of this guidance

Overloaded networks, flooded email systems, large and complex record formats, a multitude of mandatory recordkeeping rules to comply with, system change and continual technological obsolescence – those managing digital records have a lot to deal with. To complicate matters further, all the problems associated with digital records have to be dealt with now. You can't defer the problem of their management because doing nothing about your digital records will consign them to oblivion just as surely as doing the wrong thing. This guidance is intended to help you get control of your digital records and manage them effectively.

Digital records will only have value for your organisation if they are accessible and if you can preserve their authenticity and integrity.

To maintain digital record authenticity, integrity and accessibility you should try to:

1. make digital recordkeeping achievable for your organisation
2. keep your digital records in recordkeeping systems
3. implement and maintain metadata about your digital records
4. effectively manage the migration of your digital records, and
5. target specific record formats that are causing you problems.

Acknowledgements

State Records would like to acknowledge the kind assistance of a number of people in the production of this guideline including: Neil Bateman, University of Sydney; Michael Carden, National Archives of Australia; Robyn Gamble, National Archives of Australia; Chalinder Hughes and team, Department of Services, Technology and Administration; Tony Leviston, NSW Department of Commerce; Matthew Lipscombe, DocBanq; Glen Morgan, NSW Treasury – Office of Financial Management; Greg Moss, National Film and Sound Archive; Peter Newman, Office of Transport Safety Investigations; Gregory Punshon, Gosford City Council; Robert Pymm, Charles Sturt University; Dawn Routledge, NSW Fire Brigades; Emma Scott, Tourism NSW and State Records' Digital Records Advisory Group

1. Make digital recordkeeping achievable for your organisation

1.1 Share responsibility for managing digital records

Managing digital records is not all up to one group of people. It requires a number of stakeholders to work in partnership.

Those responsible for information technology and records management in your organisation need to work together to ensure that the infrastructure, systems, policies and procedures are in place to support the capture of digital records and their metadata. Such partnerships will also help to ensure the maintenance of these records, with their essential characteristics unchanged, for as long as they are required. Key roles in your organisation are outlined in State Records' *Policy on digital records preservation* at http://www.records.nsw.gov.au/recordkeeping/policy_on_digital_records_pres_14381.asp.

1.2 Limit the number of file formats used in your organisation

It is estimated in the business environment that 4500 types of record formats exist today. It greatly simplifies the management of digital records and minimises costs if you identify a minimum set of formats which meet business needs and longevity concerns and restrict data creation to those formats.

Example of how choice of file formats can affect your organisation:

Organisation 1 limited the number of file formats staff could use. It had 5 in common usage. This ensured they could easily manage the digital preservation process.

Organisation 2 did not limit the file formats staff could use. As a result it had over 30 file formats in common usage. These included digital video, information graphics and various other forms of multimedia publishing. Due to the large number of formats to cater for, digital preservation, in particular migration, was significantly more complex and costly.

1.3 Use open formats

Seek to use 'open formats' ie those that are:

- based on open standards ie the full specifications of standards on which the format is based are freely available
- developed by a community rather than particular vendors or interest groups
- supported by multiple software implementations created by different authors
- not the subject of intellectual property or patent restrictions.

Such formats are less at risk of becoming inaccessible because of changes to vendor arrangements and are easier to migrate.

Examples of open formats:

- PDF/A-1, the 'archival' format for PDF. PDF/A-1 has fewer "bells and whistles" than traditional PDF which minimises future migration requirements. PDF/A-1 is more open than traditional PDF because it is maintained by the International Standards Organisation, not one specific vendor
- OpenDocument Format (ODF), an open XML-based document file format for office applications to be used for documents containing text, spreadsheets, charts, and graphical elements

- Hypertext Markup Language (HTML)
- Extensible Hypertext Markup Language (XHTML), a version of HTML that conforms to the XML syntax and therefore allows automated processing to be performed using standard XML tools
- Joint Photographic Experts Group File Interchange Format (JPEG or JFIF), Tagged Image File Format (TIFF), Portable Network Graphics (PNG) for digital images
- Free Lossless Audio Codec (FLAC) for digital audio files.

For high value, long term records, it may be more cost effective to migrate these records to open formats shortly after their creation or shortly after their active business use has ceased. See [4. Effectively manage the migration of your digital records](#) for further guidance.

1.4 Use templates

You can make templates available to staff for the regular types of documents and records created within your organisation. Your organisational procedures should encourage staff to use them. Documents created using well-crafted templates will save time by reducing the need for staff to retype standard text or to spend time formatting. Templates can contain standard features such as fonts and styles which not only help create a uniform 'look' to departmental documents but can assist migration to new platforms. Prompts in the templates can ensure the capture of essential elements required to verify the identity and reliability of the documents. Structural or contextual information (metadata) can be created and captured in a consistent way and can enable the record to be understood well into the future. Groups of records created using the same template can be migrated easily to new systems or formats, including open standard formats, with less loss or alteration of content, which may promote large scale preservation. The use of templates is also beneficial to the quality of XML generated when documents are converted to this durable file format for long term preservation.

1.5 Apply standard creation rules

Creation practices can either promote or endanger the long term preservation of records. Having clear, uniform record creation standards that all users follow will help you to maintain accurate, authentic and accessible digital records. Ad hoc or idiosyncratic practices will make the challenge of digital preservation significantly harder.

Some creation practices can be built into your organisational templates. Your organisation may choose to familiarise staff with certain creation practices or build them into business processes which produce records required in the long term.

Below is a list of creation 'rules' for end users when creating word processed documents, emails and spreadsheets and some further resources which provide rules regarding images. These rules should be considered best practice, particularly when creating records that are likely to be retained in the long term (ie over seven years) or as State archives. Once records are created they should be saved into recordkeeping systems as soon as possible.

Word processed documents¹

Always begin with an empty template

Do not create a new document by changing an existing document based on the same template. Templates often include metadata regarding context. Copying an existing document means you may save incorrect metadata from the original document to the new document or risk that not all relevant new metadata will be completed. You can verify information displayed in the Properties window if required.

Use styles to impart structure to documents

Format styles in templates (eg Heading 1, Heading 2, Heading 3) impart structure to documents which not only increases standardisation and readability, but also helps preserve meaning.

Exercise restraint when copying and pasting sections of text with different formatting

If you copy and paste text into a template with different format styles the styles will be added to the template. This can cause problems when preservation actions are carried out.

Do not use passwords to protect documents

If you forget your password you will not be able to open the document and the information will no longer be accessible. Passwords for editing the document can be set, however, and do not compromise the digital sustainability of the document.

Use standard fonts

Unconventional fonts can be lost in migrations and reduce the probability of authentic preservation of word processed records.

Use headers and footers to include suitable metadata (information)

Headers and footers are ideally suited to the capture of metadata such as the name of the file, version number, date etc. Prompts to record this information can be built into templates.

Avoid date/time insert fields

The automatic capture of dates and times in templates is undesirable as they are updated every time the document is opened. The only automatic date field which may be suitable to use is Print Date. If used, it should clearly indicate it is the last printing date.

Insert any images or illustrations in suitable formats

Images and illustrations should be inserted in formats that are more likely to be preserved in the long term, eg TIFF. See *Managing born digital images – still photographs* for more information.

Do not use text boxes when a table would be more appropriate

Many documents use spaces to vertically align information into columns but during migration this layout could be lost. The best way to create columns is to use a table or a specific alignment.

Use the indent functions instead of spaces

Spaces may be lost during a migration.

¹ This section is drawn from Digital Preservation Testbed, *From digital volatility to digital permanence*, Part 3, Preserving text documents, pp.48-52, viewed June 2008, <<http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-textdocs-en.pdf>>

Give preference to object embedding over linking

The information contained in linked objects is only updated when changes are made to the source file. The target file only stores information about the location of the source file and displays an image (icon) of the linked file. Linked objects should only be used when it is necessary to restrict file size. If using links, the link between the source and target file should be removed when the text document has acquired its definitive form and can no longer be changed.

Embedded objects are incorporated as part of the target file. With an embedded object, the information in the target file is not changed when the source file is changed because the object no longer makes use of the source file.

Emails²*Always use the address book in your email application*

The address book contains extra information about the people to whom you are sending messages. This information is stored together with the email message for context. Address book information should be filled in as completely as possible.

Be careful when using distribution lists for email messages if addresses are needed to provide contextual information

Names and address and other details of recipients of emails are not always registered on distribution lists. Depending on the email application and type of email, the name of the list and people on the list will not appear in the email. Distribution lists are dynamic (ie names are added and removed constantly) and it is nearly impossible to tell who is on a distribution list at the particular time and email was sent.

Information about who the email is being sent to can be added to the text of an email sent via a distribution list. Whether this is necessary depends on the information being sent and the importance of knowing who is receiving it eg if you are circulating a draft you may need to prove it has been sent to all relevant people for their comment before being released.

Always give email messages a subject

This is contextual information and enables the email to be sorted and evaluated by recipients. The subject line should be relevant and useful.

Only add 'flags' to messages such as urgency or sensitivity flags when necessary

Although flags can be useful, not all email applications can reproduce them correctly and they may not be seen by the recipient. It is better to include this information in the subject line or body of the message.

Wherever possible make and send email messages in plain text or HTML

Messages in plain text are suitable for simple emails. More formal and official emails eg with images or logos can be made in HTML. Beware of using Microsoft Outlook's Rich Text Format (RTF) because this is specific to Outlook and when sent is coded in a file that may contain attachments and layout information. This data has to be translated to be read by other email applications. MS Exchange does this translation and what is sent depends on the Exchange settings.

Do not use automatically updating fields in email messages

² This section is drawn from Digital Preservation Testbed, *From digital volatility to digital permanence*, Part 4, Preserving email, p.74-79, viewed June 2008, <<http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-email-en.pdf>>

Always enter this information as 'hard' text. Automatic fields are unstable and may update every time you open an email causing the content and context of the email to be lost.

Seek to send attachments in open formats

For example, an image can be sent as a bitmap or a JPEG file. Do not paste images into an application like MS PowerPoint or Word. These applications produce files in proprietary format while most viewers can render bitmap or JPEG.

When replying to an email message do not insert text into the original message

If you wish to respond add your comments at the top above the headers of the original message. This will keep your comments separate from the original. Do not forget your email may be read by someone in twenty or thirty years time when you cannot explain what you added.

Use a signature block

This provides important contextual information about you as the sender. It is worth using two signature blocks: one for internal emails and one for external use for more official correspondence. Internal signature blocks should contain name, position, project or department, organisation. External signature blocks should also contain: address, telephone number, email address and website.

Spreadsheets³

Always begin with an empty template

Do not create a new document by changing an existing spreadsheet based on the same template. Templates often include metadata regarding context. Copying an existing document means you may save incorrect metadata from the original document to the new document or risk that not all relevant new metadata will be completed. You can verify information displayed in the Properties window if required.

Do not use passwords to protect spreadsheets

If you forget your password you will not be able to open the spreadsheet and the information will no longer be accessible. Passwords for editing the spreadsheet can be set, however, and do not compromise the digital sustainability of the document.

Use standard fonts

Unconventional fonts can be lost in migrations and reduce the probability of authentic preservation of spreadsheets.

Use headers and footers to include suitable metadata (information)

Headers and footers are ideally suited to the capture of metadata such as the name of the file, version number, date etc. Prompts to record this information can be built into templates.

Assign meaningful names to rows and columns (titles or labels)

This provides important contextual information to the spreadsheet to enable it to be understood, even with the passing of time.

Avoid automatic date and time functions like "=NOW()"

The result of the NOW() function is the current date and time in the form of a serial

³ This section is drawn from Digital Preservation Testbed, *From digital volatility to digital permanence*, Part 2, Preserving spreadsheets, p.50-53, viewed June 2008, <<http://www.digitaleduurzaamheid.nl/bibliotheek/docs/volatility-permanence-spreadsh-en.pdf>>

number that is automatically recalculated each time the spreadsheet is opened, which is undesirable.

State currency in a separate cell and in full

When making use of currency amounts state the relevant currency in the title or name of the column. An integrated currency symbol eg typing \$AUD1,000 into a column can be lost in migration or replaced by a different currency symbol.

Images

For further information regarding standard creation rules for images see:

- The section of these guidelines [5.2 Managing 'born' digital images - Still photographs](#) for advice regarding born digital images.
- General Retention and Disposal Authority - *Imaged records* (GDA24) at <[http://www.records.nsw.gov.au/recordkeeping/imaged_records_\(gda_24\)_9260.asp](http://www.records.nsw.gov.au/recordkeeping/imaged_records_(gda_24)_9260.asp)> for retention and disposal advice concerning imaged records.
- Recordkeeping in Brief 11 - *Digital imaging and recordkeeping* at <http://www.records.nsw.gov.au/recordkeeping/rib_11_digital_imaging_and_recordkeeping_801.asp> for technical specifications and tips for creating quality scanned images.

1.6 Destroy digital records when appropriate

Investment by your organisation in the preservation of digital records should be made based on an understanding of how long the records must be retained.

Tip: Not destroying records will cost you lots of money

Beware of those who argue for keeping all digital records because storage is cheap. While this may be so:

- preserving records is expensive! Public offices have an obligation to maintain accessibility to equipment/technology dependent records under s.14 of the *State Records Act* and a business need to have accessible information. Maintaining accessibility over time is an expensive undertaking and should only be considered for records that are truly needed and are required to be kept for long term retention or as State archives
- some records should be routinely destroyed as authorised e.g. those containing personal or sensitive information in order to respect the rights of individuals and comply with privacy laws⁴
- retaining records unnecessarily leads to information confusion - staff are presented with too many hits for each information request. This can result in loss of productivity as staff try to filter information requests and find the

⁴ The *Privacy and Personal Information Protection Act 1998* (NSW), Principle 5, s.12 states that 'a public sector agency that holds personal information must ensure: (a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and (b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information'. The *Health Records and Information Privacy Act 2002* (NSW), Schedule 1, s.5 indicates that (1) An organisation that holds health information must ensure that: (a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and (b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information.'

most relevant information

- retaining records unnecessarily can also inhibit the ability to locate and retrieve information quickly and efficiently for Freedom of Information requests, Discovery Orders
- retaining large numbers of digital records may reduce server speed resulting in a user response lag time
- at some point, even with cheap storage, information will need to be deleted to improve performance and make way for new records. If you have not tagged records from their creation with authorised disposal information, the process of deciding what to delete will be labour intensive and difficult.

Knowing how long records need to be retained can help your organisation to make decisions about creation (eg formats to use) and can also assist you in planning preservation activities. For example, clearly it is not necessary to invest a lot of time and energy into a preservation activity such as the migration of a group of records to a new more sustainable long term format if they are due for destruction. Likewise it is not necessary to develop templates and detailed work practices for areas of your business where records are kept for only one year after audit.

In order to know up front which digital records will need to be kept for long periods of time, identify the retention periods for records. This means ensuring that digital records are covered by authorised retention and disposal authorities and sentence the records using those authorities.

Further assistance:

For an introduction to the retention and disposal requirements in the NSW public sector see Recordkeeping in Brief 48 - *Disposal at a glance* at http://www.records.nsw.gov.au/recordkeeping/rib_48_disposal_at_a_glance_13684.asp.

Digital records that do require destruction should be destroyed in a manner that it irrevocable – to ensure that they cannot be reconstituted.

Further assistance:

For further information about total destruction of digital records see Recordkeeping in Brief 51 - *Destroying digital records: When pressing 'delete' is not enough* at http://www.records.nsw.gov.au/recordkeeping/rib_51_destroying_digital_reco_15307.asp.

1.7 Implement a 'technology watch'

Digital records are particularly vulnerable to obsolescence. It is necessary for all organisations with digital records to mount a 'technology watch' to monitor their condition and the ongoing viability of the systems that they are contained in or the support for the format they are stored in. This will require you to be aware of the systems and formats used within your own organisation and to be alert to changes by vendors, forthcoming obsolescence, impending withdrawal of vendor support or other factors that may affect organisational systems and digital resources.

There are a number of tools and resources that can assist with monitoring digital records for obsolescence and therefore facilitate migration.

Examples of tools and resources:

- The Automated Obsolescence Notification System (AONS) is a tool, developed by the National Library of Australia and the Australian Partnership for Sustainable Repositories, which periodically analyses digital repositories and determine whether any digital objects within them are in danger of becoming obsolete. It then sends notification reports to the repository manager. For more information see <<http://www.apsr.edu.au/aons>>.
- The National Archives of United Kingdom has an online registry of technical information called PRONOM which gives advice regarding file formats, software products and other technical components required to support long term access to digital records. For example, PRONOM can be used to monitor the file formats held in an archive and to maintain information on the status of each file format eg which application is able to understand and render the file format, on which hardware platforms the application software is available, whether the application is still supported by the manufacturer etc.⁵ For more information see <<http://www.nationalarchives.gov.uk/pronom/>>.

1.8 Plan for the costs of digital preservation

As part of planning it is important that you allocate adequate resources for digital preservation. Costs of digital preservation will vary according to the strategies chosen, past and present controls and the complexity of the digital environment. Careful planning can help you to reduce costs significantly.

Examples of how to reduce costs:

If your organisation has implemented tight controls regarding the creation of records in standard, limited formats using specifically designed templates then the cost of long term preservation will be lower than those for an organisation without those controls.

If your organisation only uses simple digital records, it is easier and cheaper to preserve them. Complex digital resources, e.g. multimedia objects, will be more expensive.

If your organisation has an active appraisal and disposal program for both paper-based and digital records, this will ensure that resources are not wasted on preserving digital records which are not required in the long term.

Costs of 'digital archaeology'

'The biggest cost...is trying to 'clean-up' or 'work-up' digital resources which should have been cleaned up or worked up at the time they were created. The creators of a digital resource are best equipped to validate it and to document it. If they do not do this then the cost of 'clean-up' at a later stage when most of the context will have been lost is conservatively estimated to be ten times greater.'⁶

⁵ Digital Preservation Testbed, *Functional requirements for a preservation system*, The Hague, n.d. p.11, , viewed June 2008, <http://www.digitaleduurzaamheid.nl/bibliotheek/docs/Technical_and_Functional_Requirements.pdf>

⁶ T Hendley, *Comparison of methods and costs of digital preservation*, British Library research and innovation report 106, Yorkshire, 1998, section 5.1.2.3, viewed June 2008, <<http://www.ukoln.ac.uk/services/elib/papers/tavistock/hendley/hendley.html>>

When budgeting for digital preservation you may need to consider the costs of:

- employees with appropriate expertise to manage projects and the training they may require
- planning, policy and procedure/guideline development and the development of templates, training etc to promote good practice and monitoring/correcting creation practices (which is likely to save costs in the long term)
- validating the authenticity of the digital records, adding adequate documentation (i.e. metadata projects) if it is not supplied at creation and managing the documentation over time
- assessing the data structure and making changes to the way digital records are formatted, compressed and encoded
- digital storage including maintenance of hardware and software and backups
- refreshment and replication of removable media, including checking for authenticity
- regular audits of online and offline digital records
- monitoring of environmental conditions for the storage and maintenance of digital records
- migration strategies/conversion to standard formats including checking for authenticity
- enabling digital records to be discovered and accessed
- rights management
- protecting digital records and keeping them secure.

Aspects of digital preservation impact on a number of business areas and will overlap with some existing costs e.g. equipment, system usage, storage, maintenance and backup costs, costs of access etc. Digital preservation will therefore involve a variety of stakeholders. Working with those stakeholders and ensuring they are aware of the impact of their decision-making can help you to streamline resources. A collaborative venture between organisations may also be a proactive way to reduce costs.

Costs can be seen in light of the value of digital resources and information assets, relative benefits of managing them over time and the risks if information is lost.

Remember: Your information (including digital records) is one of your organisation's greatest assets. The NSW Government recognises this and encourages all public offices to manage their information efficiently in order to safeguard this asset and derive the most benefit from it. For more information see the Government Chief Information Office's statement - *Information as an asset* at <<http://www.gcio.nsw.gov.au/ict-key-strategies/information-management-1/information-as-an-asset>>.

1.9 Use removable media only when you have to

Some organisations use removable storage media (or offline storage) to store records away from active systems. This approach, however, is risky.

It is preferable to consider storing long term or archival digital records on either networked servers or online spinning disc storage systems rather than removable media such as optical disks (eg CD-Rom, DVD) or magnetic media (eg magnetic tape, floppy disks).

Online spinning disc storage systems are as economically viable as removable media and are inherently a more stable medium for long term storage.

An example of online spinning disc storage systems is RAID. RAID (redundant array of independent disks) is an umbrella term for computer data storage schemes that combine two or more physical hard disks into a single logical unit by using either special hardware or software. When several physical disks are set up to use RAID technology, they are said to be *in a RAID array*. This array distributes data across several disks, but the array is seen by the computer user and operating system as one single disk.

Records on removable media tend to be at higher risk as:

- they tend to be easily ignored or forgotten while online systems are more readily monitored
- there is the potential that they can be damaged (eg through handling and use or through media degradation) or lost
- they have no centralised backup.

Case study: Be aware of what you have stored on removable storage media and look after it carefully

One organisation used a large quantity of removable storage media to store records that it needed to keep long term. The storage media used were not clearly labelled and they were stored together with the organisation's backup tapes. After several months staff forgot what was actually on these storage media and they were included in the cycle of backup tapes. The data they contained was quickly overwritten and the records that had long term value to the organisation were lost. As they were not on the server there were ironically no backups available.

If you use removable media, make sure you look after it

If records need to be stored on removable media, they should be:

- stored in appropriate conditions (eg magnetic media should not be in close proximity to magnetic fields or heavy-duty motors; stable temperature and humidity should be maintained, areas should be low light, dust, moisture etc)
- stored in suitable packaging and storage containers for their protection
- accurately labelled and should contain all metadata necessary to explain the content, context and management of the records contained on the media.

Consideration should be given to keeping validated copies in an alternative location (for disaster recovery purposes) and the media should be monitored regularly for signs of degradation or obsolescence. Procedures should be in place and promulgated to all staff to ensure that digital records on removable media are:

- handled carefully, and
- only accessed by authorised personnel.

Monitor removable media

Monitoring digital records on removable media may involve:

- checking optical media (eg CDs and DVDs) to see if they are scratched or dirty, or if the layers are flaking, changing shape or corroding

- checking magnetic media (eg magnetic tape, floppy disks) to see if the tape is brittle, flaking, separating or blocking together, mouldy, dusty or there is 'print through' from one layer to another
- ensuring protective packaging and storage containers are protecting the media effectively
- ensuring handling and access rules are being followed, particularly for records of long term value
- regularly 'exercising' magnetic media to prevent creases or folds forming in storage.

Monitoring should also include:

- ensuring that magnetic media have not been placed in proximity to heavy duty electronic motors, such as those in some air conditioning units, or magnetic fields
- preventing large fluctuations in temperature and humidity or extremes of either, exposure to excessive sunlight or UV light, moisture or dust in storage areas for physical media or servers.

Refresh and replicate storage media where necessary

If your organisation stores digital records on removable media, you will need to consider migration, refreshment or replication to mitigate risks associated with the formats.

Refreshment (or copying) is where the data is transferred unchanged from one medium to another of the same type, for example, copying data from one CD-Rom to another CD-Rom.

Replication (or reformatting) is where data is transferred unchanged from one medium to another of a different type, e.g. copying data from a hard drive to a CD-Rom. Replication does not alter its physical representation or intellectual content.

Refreshment or replication should be performed when media is becoming outdated and new storage devices and media are being installed or at a pre-established point in the life expectancy of the storage medium, such as half its projected life expectancy. It should be a priority if degradation of the media is already evident.

State Records does not require organisations to treat refreshment or replication as a form of migration, so these processes are not subject to the stringent conditions outlined in the General Retention and Disposal Authority – *Source records that have been migrated* (GA33) at <http://www.records.nsw.gov.au/recordkeeping/source_records_ga33_15630.asp>. However, refreshment and replication should be performed with care and diligence as they can alter records and compromise their authenticity.

Refreshment and replication practices should include:

- a quality control procedure that mandates the validation of the accuracy of copied records e.g. visual comparison of several reformatted records with their old formats, comparison of checksums to confirm no changes have occurred
- documentation of all steps involved including all persons involved, the date performed and format of the data.

Any superfluous copies of records that remain after refreshment or replication is successfully complete may be disposed of under Normal Administrative Practice (NAP).

Tip: Avoid significant quantities of removable media

One problem you may encounter with removable media is that their sheer quantity becomes unmanageable over time. Eventually you may have too much media to renew within the time span that you have to renew it, making refreshment and replication less viable options. Eventually there will come a point where you cannot refresh or copy fast enough to keep up with obsolescence. Having to change data formats as well as media compounds the problem immeasurably. The move to normalisation and isolated online systems for storage may be a more viable long term solution.

Further assistance:

For more information about the storage of physical media see Guideline 11 - *Solutions for storage: Guidelines on the physical storage of State records* at <http://www.records.nsw.gov.au/recordkeeping/guideline_11_solutions_for_storage_5041.asp>.

For information on the storage of magnetic media and optical disks see the National Archives of Australia's, *Frequently Asked Questions*:

- *How do I protect and handle magnetic media?* at <<http://www.naa.gov.au/records-management/secure-and-store/physical-preservation/faq/magnetic-tape.aspx>> and
- *How do I protect and handle optical disks?* At <<http://www.naa.gov.au/records-management/secure-and-store/physical-preservation/faq/optical-disks.aspx>>.

© State of New South Wales through the State Records Authority, February 2009. This work may be freely reproduced and distributed for most purposes, however some restrictions apply. See the copyright notice on www.records.nsw.gov.au or contact State Records.

ISBN: 978-0-9805148-9-6