Sample procedures for staff: managing shared drives

Note: This is a sample procedure for staff explaining how they should manage their shared drives. It requires modification by organisations to reflect their unique situations and business practices (i.e. instructions in blue writing & square brackets). *Advice XX: Managing shared drives* provides further information about how to manage this important resource and ensure the organisation's recordkeeping requirements are met.

What are shared drives?

Shared drives, also known as network drives, are used by [our organisation] to store electronic information, including Word documents, Excel spreadsheets, PowerPoint slides, digital photos, PDF documents and database reports.

For convenience in this advice, 'document' is used to refer to all of these information types.

The shared drives used in [our organisation] include:[delete any that do not apply]

- Organisation-wide drive [X drive]: This drive if for information that needs to be shared across the organisation as a whole.
- Workgroup drives [Y drive]: These are established for a business unit or for a particular project and are accessible to those within the unit or project only.
- Personal drives [Z drive]: These are created for each user and accessible only to the user.

What are the advantages of shared drives?

Shared drives are part of [our organisation's] information strategy. Shared drives are used because they have many business benefits for [our organisation]. For example:

- digital information is easily accessible to those who need to refer to it, and can be easily reused
- digital information is backed up and recoverable in the event of system failure
- users can refer to documents in a central location rather than managing or emailing duplicate copies, saving storage space.

What are the disadvantages of shared drives?

There are a number of risks in using shared drives, however. These include:

- difficulty in locating, retrieving and using information if the drive has not been structured or titled appropriately
- insecurity of information: while some security measures can be added, most information on shared drives can be easily edited or deleted and there are no audit trails
- records stored only on shared drives cannot be used as evidence by the organisation as their authenticity may have been compromised
- information accumulates and is rarely deleted, leading to volumes of storage that are costly to maintain.

Business rules for using shared drives

To ensure that shared drives are used in a manner that maximises the business benefits and minimum the risks and costs to [our organisation], users are asked to implement the following business rules.

1. Save your documents to the correct drives

Personal drives (the [Z drive]) have been provided for you to store your personal documents [indicate if size limit on this drive]. Never use this drive for the storage of information of corporate value as it is inaccessible to others. Note [our organisation's] code of conduct [and/or appropriate use ICT policy] with regard to keeping non-business information.

All corporate information, even documents that only you need to access, should be saved to the [X] or [Y] drives. No personal documents should be saved to these drives.

Examples of documents you should save to these drives:

Personal drive	**Workgroup drive**	**Organisational drive**
Your Resume Professional/career information Copies of your training and development records for your reference Documents unrelated to official business	Corporate information that can be ***shared with the workgroup*** including: • Research, drafts and final versions of documents, reports, minutes etc for a project or business initiative carried out within the workgroup or business unit • Administrative matters associated with the workgroup or business unit e.g. flexitime sheets • [add business specific document types appropriate for sharing across workgroups/business units here]	Corporate information that can be ***shared with the whole organisation*** including: • Research, drafts and final versions of documents, reports, minutes etc for projects or business initiatives that involve staff across workgroups and business units • Organisation-wide policy and procedures • [add business specific document types appropriate for sharing across workgroups/business units here]

2. Structure your shared drives

It is essential that organisation-wide and workgroup drives are logically and hierarchically structured so that information can be easily retrieved and used by others.

[Choose either 2A or 2B here, as appropriate. 2A is suitable for small, centralised organisations with centralised structuring and management of drives and 2B for larger, devolved organisations where workgroups may be developing and managing their own drive structures].

2A

In [our organisation] we have set up our network folders according to.. [Explain structure of organisation-wide and any workgroup drives. If the organisation has a standard classification scheme or thesaurus that users are expected to follow describe this here. More detail or reference to classification guidance may be required.]

This structure is maintained by.. [who is responsible for creating, deleting folders.]

2B

In [our organisation] we have set up our network folders according to.. [Explain structure of organisation-wide and any workgroup drives. If the organisation has a standard classification scheme or thesaurus that users are expected to follow describe this here. More detail or reference to classification guidance may be required.]

This structure is maintained by.. [who is responsible for creating, deleting folders.]

If your workgroup (business unit or project) does not have a structured drive [and there is no organisation-wide classification scheme to emulate], your group will need to devise a suitable structure based on the business activities you perform.

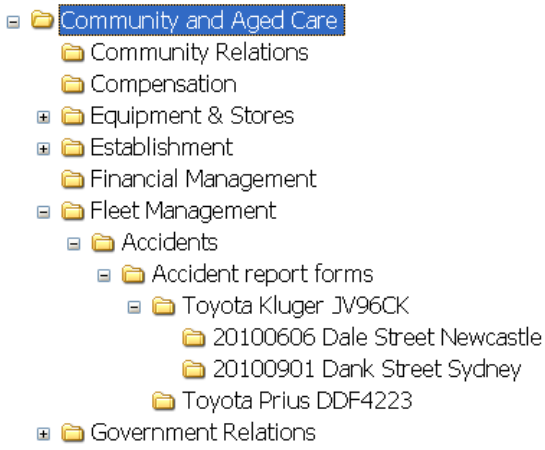
Tips:

- The structure of the drive should consist of a series of folders that group information used by the workgroup.
- Each folder should have a title that accurately reflects the content of the folder e.g. areas of business activity. Do not title folders using individual names or position titles.
- Each folder should be differentiated from others by its title so it is clear where information should be saved.
- Sub-folders may be used for subsidiary business activities, but the number and level of sub-folders should be limited to prevent confusion and promote clarity.
- Limit repetition in the titles of folders and their sub-folders. Consider the titles of a folder in the context of the whole path.
- Security restrictions should be attached to folders or documents where required.

One person in the workgroup should be allocated as an administrator, with responsibility and permission for setting up the structure, adding or deleting folders in accordance with business needs, assigning security and monitoring and auditing use of the structure. This person can provide training to their workgroup, including induction for new staff in how to use the structure.

Examples:

This is an example of such a structure for administrative matters drawn from the organisation-wide share drive of the fictional Community and Aged Care Department. [Note: This is based on Keyword AAA or Keyword for Councils hierarchies. If these are not used, replace the example with the classification structure type used within the organisation, or develop one according to needs].



This is an example of a structure designed for a business area that handles large scale procurement. The structure reflects the process stages. [Could replace with business-specific example]

For information or assistance in establishing shared drive structures or moving existing information to structured shared drives, consult [records or information manager].

3. Use naming conventions for folders and documents in shared drives

To promote retrieval and sharing of information, it is also essential to use good naming conventions (standard rules) for folders, sub-folders and documents.

Use the [organisation's] standard terminology [mention classification scheme/thesaurus/conventions if they exist] and forms of names for organisations and people, names of projects and activities, dates etc in folder and document titles.

Examples of file titles

File note re contract negotiations with Aurora Corporation

20100909 Minutes of Industry Focus Group

Managing Digital Records v1.2 DRAFT

Further rules

- Use standard common terms across units e.g. budget, progress report
- Use standard names for document types e.g. minutes, memorandum, leaflet, file note, policy, project plan. [Note: State Records' Document form scheme provides a standard list that might be used or adapted].
- Don't add descriptions such as 'presentation' or 'spreadsheet' to document titles as the document extension describes these already.
- Avoid using technical jargon and acronyms which make retrieval difficult, particularly over time.
- Use the convention YYYY/MM/DD to display dates e.g.20101010. If documents need to be arranged by date, place this first in the document title
- Use the convention Surname, First name to display names if documents need to be arranged in alphabetical order by surname
- Note: Remember not to duplicate information in the title of folders – the folder path will give the business context.

Example [replace with organisation specific example]

Use: Compliance/Breaches/Investigation reports/20091201 Endeavour Pty Ltd

Not: Compliance/Breaches of compliance/Investigation reports/20091201 Investigation into Endeavour Pty Ltd

4. Control versions

It is valuable to distinguish versions of documents by including a version number in a document's title. This enables you and others to clearly track which version is which.

A common method of expressing versions is to use v1.0, v2.0, v3.0 etc for approved and issued versions of documents and the decimal to distinguish drafts that are made between versions (e.g. v1.1, v.2.5, v3.2).

It is also good practice to include the document title and version in the footer of the document itself [indicate if this is built into organisational templates].

For clarity it is valuable to add the status of the document (whether draft or final) at the end of the title.

Example:

Report on survey of mining practices 2010 v2.1 DRAFT

Report on survey of mining practices 2010 v3.0 FINAL

5. Use appropriate security on shared drives

Organisation-wide folders are, by default, open to all users. Workgroup folders are restricted to particular workgroups.

Some folders and documents stored on shared drives will require additional security protection including password protection, specific access controls or encryption as well as sensitivity labelling. These should be in line with the organisation's security strategy and classifications. Contact the [Administrator for the organisation or workgroup or the relevant records manager or ICT manager responsible for shared drives] to add suitable restrictions.

In some cases, it may be inappropriate to store sensitive, confidential or personal information on shared drives. If in doubt, check [the organisation's] business rules.

6. Ensure records of corporate value are saved to corporate recordkeeping systems

Shared drives should only be used for records in the short term – in drafting, editing and sharing documents. They do not have sufficient controls to manage records appropriately. For example, they cannot adequately protect records from unauthorised access or deletion, they do not place records in context with other types of records regarding the same business matter, and their use cannot be adequately tracked.

As a result, it is each user's responsibility to save records of their business to the organisation's [corporate recordkeeping system/s – indicate what this is e.g. EDRMS, printing to paper] where they can be protected appropriately as managed as reliable evidence of business. The [records management procedures] indicate how to save to the [corporate recordkeeping system]. If in doubt, contact [records or information manager].

Tip: If you are emailing a document on the shared drive to others for comment or action, this may be a suitable time to capture them as record into corporate recordkeeping systems.

You should be guided by [the organisation's] records management policy / procedures and business rules for your workgroup regarding what you need to save to corporate recordkeeping systems.

[Note: If the organisation does not have a digital recordkeeping system they need to consider whether there are business needs to retain some records in digital form as well as printing and filing the 'record' copy. This might involve saving records to a read-only drive on the network.]

Not all documents in shared drives will need to be saved to the corporate recordkeeping system.

For example:

You may have saved some copies of journal articles or reports from external sources to the shared drive for your information and these are no longer needed.

You may have some working papers that have no further use to the organisation once the report has been finalised.

You may have some duplicates, records that have already been saved into the corporate recordkeeping system or insignificant drafts of letters or documents that are no longer required.

[Add guidance for users on what can be routinely deleted under guidelines for your organisation – if appropriate refer to organisation's guidelines / RM policy]

If you have captured your records to corporate recordkeeping systems, the shared drive copies can be deleted (or moved to read-only drives) when no longer required.

7. Prevent the storage of duplicate files

You can assist the organisation to reduce storage space and duplication of files by adhering to these simple rules.

A. Title your documents according to the same conventions so that the same file is not saved under different titles by different users.

B. If a document is required as a record, instead of attaching a document you have on the shared drive to an email destined for a number of internal participants, save the document to the (digital) corporate recordkeeping system. Then provide by email a link to where the document resides in the corporate recordkeeping system. Refer to [records management procedures] for how to do this.

[If the organisation uses a document management tool (e.g. document management in TRIM or Objective or stand-alone tools) to draft and circulate for comment or check in/check out functionality of document management packages explain how these are to be used.]

[Alternatively if the organisation does not have a digital recordkeeping system:] Instead of attaching a document you store on the shared drive to an email destined for a number of internal participants, provide a pointer in the email to the shared drive copy. You will need to print and file the document and the email together to your paper recordkeeping system as evidence of what you sent. Refer to [records management procedures] for how to do this.

C. If documents are attached to an email from people external to the organisation, and they need to be saved and edited, you should only (i) save an unedited copy of the email and attachments to the corporate recordkeeping system (ii) save a copy of the attachments to the shared drive for editing if you are the prime recipient. No other recipients should save them.

D. If documents are attached to an email from an internal source, you should only save the email and attachments to the corporate recordkeeping system or make attachments available on the shared drive for editing if you are the sender.

E. When saving documents shared by multiple recipients to the corporate recordkeeping system, you should search first to ensure they have not already been saved. Good titling and version control by all users will assist in this regard.

F. If you have created 'ZIP' files for emailing information, regularly delete these from your shared drives. These are always duplicates and you should have saved the record already.

8. Perform regular housekeeping of your shared drives

It is important that regular 'housekeeping' is conducted to keep shared drives in good order and promote ease of retrieval.

Folders

Maintenance of folders in the organisation-wide shared drive will be managed by [position title/s with responsibility].

The person assigned with responsibility for managing folders in each workgroup should regularly review folders to ensure they meet business needs.

Documents

Each user is responsible for managing the documents they create. When you have completed publications, projects, or stages of projects, or particular business responsibilities you will need to examine your documents on the shared drive and ensure that:

- records have been saved to corporate recordkeeping systems in line with business rules
- documents and ZIP files you created that no longer have value for the organisation are deleted in accordance with organisational procedures.

If some documents need to be retained for longer periods, you will need to review them at a later date.

Note: If the documents are being edited or used by a number of users, one person within the group needs to take on responsibility for managing their fate. For example, the project team leader.

If you are moving from one workgroup to another, or exiting the organisation, you will need to ensure that the above responsibilities are met (or the responsibility for documents that need to remain in the shared drive is transferred to another officer) before you leave. You will also need to empty your personal drive.

These measures will prevent the unnecessary accumulation of storage in the organisation.

Further assistance

If you would like further assistance or have any questions contact [records or information manager].