Module 3: Store & Protect
Introduction

By storing and protecting University information throughout its lifecycle you will ensure it is able to be accessed for as long as required by you, your colleagues and the University.

All staff members at Curtin are responsible for ensuring that original University documents are created and stored appropriately, particularly those of continuing or historical value.

On successful completion of this module you will be able to:

- Recognise where to store information at Curtin.
- Identify how to protect information at Curtin.
How do we store information?

Information at Curtin can be created in a range of formats and stored in a range of locations. It can be organised using the Curtin Common Vocabulary.

- Create electronic folders on your shared drive.
- Move University email messages to your area’s shared email mailbox (or shared drive if you do not have a shared mailbox).
- Create paper folders for hard copy University records.
- Create reference folders for copies of paper and electronic documents so they can be destroyed when no longer needed.
Where should I store electronic information?

- Always store documents within Curtin’s official Information Management System - your shared drive or shared mailbox.
- Place documents within the appropriate folders according to the Curtin Common Vocabulary.
- Do NOT store official Curtin documents on your desktop, personal drive or personal email folders.
**How do I ensure the security of information?**

Information must be classified to ensure the correct level of security. This will ensure that only staff authorised to view sensitive material have access to it.

When folders are created they should be classified according to the following security levels:

<table>
<thead>
<tr>
<th>PUBLIC</th>
<th>Information that is not sensitive.</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERNAL ONLY</td>
<td>Public release could cause harm to the University, another organisation or an individual.</td>
</tr>
<tr>
<td>______________________-IN-CONFIDENCE</td>
<td>Unauthorised disclosure, modification or destruction can be reasonably expected to:</td>
</tr>
<tr>
<td>• COMMERCIAL-IN-CONFIDENCE</td>
<td>• cause harm to Curtin, another organisation or individual</td>
</tr>
<tr>
<td>• LEGAL-IN-CONFIDENCE</td>
<td>• provide an unfair advantage to an entity</td>
</tr>
<tr>
<td>• MEDICAL-IN-CONFIDENCE</td>
<td>• violate somebody's right to privacy.</td>
</tr>
<tr>
<td>• STAFF-IN-CONFIDENCE</td>
<td></td>
</tr>
<tr>
<td>• STUDENT-IN-CONFIDENCE</td>
<td></td>
</tr>
<tr>
<td>PROTECTED</td>
<td>Unauthorised disclosure, modification or destruction can be reasonably expected to cause serious harm to:</td>
</tr>
<tr>
<td></td>
<td>• the University, another organisation or individual</td>
</tr>
<tr>
<td></td>
<td>• Australia's national security, national interest, economy, stability or integrity</td>
</tr>
<tr>
<td></td>
<td>• Australia's international relations or defence.</td>
</tr>
</tbody>
</table>
Where should I store paper information?

University information

There are five styles of folder cover used for official, University information.

![Folder styles]

These folders make Curtin's official documents more easily identifiable.

Order these folders through [Records & Information Management](#).

Ephemeral information

When storing duplicate copies for reference purposes simply use reference only folder covers so these documents can be easily identified. This makes it clear that they can be destroyed when they are no longer needed.
There is a sixth folder cover that can be used for ephemeral reference information.

**Tips for storage**

- Use official folder covers for University information.
- Ensure that all reference material is clearly marked so that it can be destroyed when no longer needed.
- Store Curtin’s documents in a secure, dust free and, if possible, temperature controlled environment.
- To find out more about protecting records in paper or other formats such as photos, tapes, maps or microfilm, check the [Care and Preservation of Paper Records](#) document.
Use the correct folders

As previously mentioned, Curtin uses a range of different coloured folders to store information according to its security classification.

Test your knowledge of the different folders by completing the following activity.

Decide what type of folder you would use to store each piece of information.

Click one of the 4 folders below to select the correct security classification of the above folder.

- STUDENT-IN-CONFIDENCE
- STAFF-IN-CONFIDENCE
- INTERNAL ONLY
- PROTECTED
How do I protect electronic information?

Always store electronic records on the shared network drives where they are backed up, accessible and readable for as long as they are required.

Beware

Do NOT store electronic records on removable media such as CD’s, DVD’s or flash drives nor place them in plastic sleeves in a file or in boxes within offices. The media will deteriorate and/or be unsupported in only a few years, making the records unreadable.
Disaster recovery and vital records

Disasters, natural or otherwise, pose a major threat to the preservation of information. However, many other minor incidents can also result in the loss of information and have a serious impact on the ability of a business or area to continue to function.

Some information is so valuable that an area would not be able to function properly or at all if it was lost or damaged. These are called vital records. It is important that you identify vital records and ensure they are protected.

Disaster recovery procedures have been developed to help you minimise the risk of disasters and to minimise the loss of information should a disaster occur. For more information read the Disaster Recovery procedures document.

If you have a disaster in your area that threatens your information in any way please contact Records & Information Management on 7050 immediately. Records & Information Management staff are trained in disaster recovery procedures and, like first aid, the faster they can respond the better the chance of recovery.

All areas must have an IT Systems/Area Disaster Recovery Plan which must also cover vital information held in both physical and electronic format. You can contact Records & Information Management for advice about completing the vital records component of this plan.

Visit Disaster Recovery Planning for more information about the preservation of vital records.

Records & Information Management can provide you with more tools and advice for storing information. To find out about our face to face training sessions, browse through the RIM Training.