FAQ ON CLOUD COMPUTING

What is the Cloud?

The 'cloud' is a broad term used to describe a service on the internet that enables information to be stored, used, edited or deleted from virtually anywhere as long as you have an internet-enabled device *(i.e. computer, laptop, tablet, mobile phone)*.

Some examples of internet cloud service providers include **OneDrive for Business (the University's approved and preferred cloud-based platform)**, Dropbox, Windows Live, Box and GoogleDrive.

Where is the data or information stored?

In most cases, the stored information is spread out across many different virtual servers that are often located in different countries. For example, Google has data centres located in the USA, Taiwan, Singapore, Finland, Belgium and Ireland.

It is also worth noting that it is the cloud service provider who chooses how or where it will store the information on its virtual servers, the user has no say in the matter.

What is Curtin's primary concern with cloud services?

Many cloud services are hosted in the USA where Australian legislation does not apply. Consequently, information that travels outside Australia is subject to foreign laws *(for example USA's Patriot Act)* and we may not have control over who can access it.

Additionally, data centres located in China, Japan, India, Singapore, Philippines and Vanuatu do not have the same data protection laws as Australia. It is for this reason that Curtin cannot guarantee that the cloud service provider can guard against the unintended disclosure of Curtin's information, and to protect the Curtin Community. Therefore, Curtin staff should avoid using cloud services that are hosted outside of Australia.

Are there any other risks that I should be aware of?

Loss of data is one of the risks associated with using a public cloud service. If the security of your account is compromised, or a system malfunction occurs, your data or information may be accidentally or maliciously deleted and removed from your account.

When this happens, the effect of the deletion will "roll out" to all of your synced devices such as computers, tablets, mobile phones, deleting all copies of your data. To mitigate this risk, it is essential that you keep copies/backups of any files in a location outside of the cloud.

What sort of data or information is suitable for storing in the cloud?

In assessing the suitability of the cloud for storing a file, you need to consider the security classification of the information it contains.

Consult the following documents for additional information:

- Information Security Classification Policy
- Decision Framework on the Use of Cloud Services
- Typical risks on Using Cloud Services

As a general rule, any files containing personal or sensitive information should not be stored in a public cloud unless it has been suitably encrypted or de-identified. Additionally, under no circumstance should files that contain “Protected” information be stored in the cloud (public or otherwise).

Who can I contact for further advice and information?

If you require further information or advice on cloud computing, you can contact the following areas for assistance:

- Information Security advice: Information Security & Assurance Team
- Legal and Contract Issues: Legal Services *(9266 2767)*.
- Technical Enquiries: DTS Service Desk *(9266 9000)*.

Please do not hesitate to contact us via phone on 9266 7050, or by email at: InformationManagementandArchives@curtin.edu.au, should you require additional assistance.

For information management advice of a general nature, you may wish to visit our website.