Sheffield Hallam University

# Cloud Storage Policy

| | |
|---|---|
| **Issuing Authority:** | Leon Etherington,<br>Acting Chief Information Officer,<br>Digital Technology Services |
| **Signed:** | on master copy July 2016 |
| **Date Effective:** | July 2016 |
| **Review date:** | May 2017 |
| **Version:** | 2016.2 |

# Cloud Storage Policy

## Objective

The University is committed to ensuring its IT Systems are secure, University data and systems are protected, and are only accessed by authorised users. All University staff using "Cloud Storage" Services must therefore adhere to this Policy.

## Definition

For this document, the phrase **"cloud storage"** refers to third party online storage services such as Google Drive, Dropbox and OneDrive. Files stored on these services can usually be accessed via any web browser and often have the capability to be "synchronised" to multiple computers and mobile devices such as mobile phone and tablets. They may also have facilities for sharing files with other people.

## Risks

Many people are now using public cloud storage in their private lives. This allows convenient access to their files and data from a number of different devices. If employed in a work context however, such services also introduce risks to the security, privacy, copyright and retention of University data. Before using cloud storage for work, users of the University computing environment must consider if the usage is appropriate and follow the policy guidance in this document to limit the risk imposed on University data.

The main risks when files are stored in public cloud storage are that:

- The University can no longer guarantee the quality of access controls protecting the data
- The location where the data is stored may not be guaranteed as remaining in the European Economic Area (EEA) or US Safe Harbour and so may not meet Data Protection Act requirements for personal data
- In many cases, public cloud storage requires that files be associated with an individual's personal account. Should that individual suddenly become ill, be absent for other reasons or leave, the University will lose access to the data
- Cloud services generally limit their liability for negligence, resulting in little or no recourse should the provider misuse, lose or damage information stored in the cloud
- Few cloud providers guarantee they will not access the information stored within their service, leading to concerns over privacy and intellectual property rights
- Some if not all providers do not guarantee that the user's ownership of the data stored in the cloud will be retained. This is primarily to enable the providers to move data around to their different server locations without your prior approval but opens further questions about intellectual property rights
- Using cloud storage client software to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal equipment
- If they have financial difficulties a cloud storage provider may end the service with little or no notice, leaving users with no access to files

## Policy Requirements

The following policy requirements aim to mitigate the risks above.

All staff have a responsibility to protect the University's data, particularly data about individuals. Staff must familiarise themselves and adhere to the following University policies, guidance and information:

***Data Protection Policy Statement***

**Data Protection Secretariat Page**

***Data Protection Guidance Note***

***Working Off-Campus: Guidance on Data and Records***

The University has provided all staff and students access to **Google Apps** and **Microsoft Office 365**. As part of this, staff members have access to both "Google Drive" and Microsoft "OneDrive for Business" using accounts based on their Staff logon ID. Microsoft and Google will store data uploaded by staff accounts in EEA or US Safe Harbour locations. Using OneDrive for Business or Google Drive via a staff logon ID is therefore the recommended Cloud Storage solution for use by University staff.

There may be some circumstances when other services and providers may need to be considered - for example when collaborating with other institutions which have a different service in place, such as Dropbox or Box.com. If other services are considered then staff must evaluate the Terms of Service for each provider and ensure that the risks above are avoided.

The following points relate to both University and externally provided services:

- Do not use cloud storage to store files containing information about individuals or other sensitive information. Refer to the University ***Data Protection Policy*** for more information.

  The only exception permitted is in the case of external collaboration, only if no other secure alternative is available. Each exception must be approved by local management and recorded. Encrypting information about individuals or other sensitive information prior to uploading is mandatory. Further guidance is available in the ***Electronic Data Encryption Policy.*** The University recommends the use of 7-Zip software, and the File Encryption functions included in Microsoft Office 2010 which are installed on all University Managed Desktop computers. The use of strong passwords on any encrypted files or folders is mandatory and is to be in accordance with the ***University Password Policy.***
- Do not use cloud storage for the long-term retention of University documents or files even for instances when you work with non-sensitive information. Use alternatives such as SharePoint and shared network drives.
  - If you are using Cloud Storage for collaboration with others, either from within the University or elsewhere, only grant access to files or folders that are required for the collaboration to take place. Access to personal data should be given on a strictly need to know basis to comply with the Data Protection Act.
- The University does not support cloud storage clients or apps, such as those available for Dropbox.
- Do not store the only copy of a file in cloud storage
- You must ensure that there is a suitable level of encryption on any mobile or portable device used to download any data about individuals from cloud storage. Such a device must be password protected.

## Scope

This policy applies to all staff, data processors, partners, suppliers and contractors and other authorised users. Any exceptions must be documented and approved.

## Implementation, guidance and good practice

The policy shall be implemented and any exceptions documented and approved on all University systems. Guidance and good practice on using Cloud Storage will be published on the IS&T Intranet site.