PROTOCOL FOR THE USE OF CLOUD STORAGE

Introduction

Cloud services are services provided by an external supplier which are made available to organisations such as the University and individuals to facilitate the sharing of files and make data available over a range of computers and other mobile devices. The terms and conditions for the use of such cloud services are defined by the external supplier. Cloud services are provided by infrastructure outside the University's own domain (data centres). Cloud storage services are usually accessed via web browsers; mobile apps; synchronisation client; drive mapping. Some examples of cloud storage providers include Dropbox, Microsoft OneDrive, Apple iCloud and Google Drive/Docs.

There are two types of cloud storage:

1. **Business services - where the contract is with an organisation/company**

Some cloud service providers offer services specifically designed for business use. Organisations contract with their preferred cloud service provider for specific services and manage the accounts for the individuals within their organisation who they wish to have access.

2. **Consumer services - where the contract is with an individual**

Consumer-orientated cloud services are often made available free of charge to individuals via a user registration process, or bundled initial hardware purchases. When signing up with a cloud service provider, the individual must accept the provider's Terms and Conditions and any associated service level agreement.

What does this protocol apply to?

The General Data Protection Regulation makes some changes to how the University and our staff can store and process information using cloud services. It is important that we act in line with these changes so this protocol sets out the requirements that must be met by the University and individual staff when using cloud storage to store or process University data.

The protocol sets out a clear definition of cloud services, specifies the types of University data for which such services may be used, and identifies the risks and measures required to reduce the risks to acceptable levels. This is in order to:

- Ensure that University employees and other partners understand the University's requirements relating to the storage and guardianship of data;
- Safeguard the security, confidentiality, integrity and availability of the University's information assets;
- Ensure compliance with national and international laws governing the storage and guardianship of data including the General Data Protection Regulation;
- Ensure compliance with contractual commitments relating to the storage and guardianship of data.

This protocol applies to all University data i.e. information which arises from University teaching, research and administration, and applies to all staff, students and other parties who have access to University data.

What are the University's requirements in relation to Cloud Storage?

The University recognises that there are circumstances where the appropriate use of Cloud services enables staff and students to work more effectively. However, these benefits must be balanced against the risks relating to processing or storing data in the Cloud.

To assess whether it is acceptable to store data on the Cloud will depend on the classification of the data it is proposed to store. The University has a data classification standard which identifies how different types of information are classified by the University.

Once you have identified the classification level of the data you propose to store on the Cloud then you must ensure your proposed storage meets the following requirements:-

Public data may be stored or processed using a cloud service which is either consumer or business-oriented. However, we recommend that you use a University supported service for all types of public data. UWS currently supports Microsoft OneDrive for Business.

Restricted, Confidential and Strictly Confidential data may only be stored or processed using a business-oriented cloud service, where the requirements of this protocol have been met. This means that the risks have been considered and addressed, the relevant areas within the University have been consulted and given their approval and an appropriate contract is in place.

Staff should be aware that certain data may be subject to specific legal or contractual requirements. For example, the NHS or funding body may require data to be stored on UWS premises, or stipulate specific security requirements. This may prevent the use of cloud services.

The responsibility for ensuring the appropriate use of Cloud services in accordance with this Protocol lies with the member of staff managing, procuring or overseeing such use.

What are the risks in using Cloud Storage?

Consumer-orientated

Consumer cloud services may involve risks to the confidentiality, availability and integrity of the data, in particular:

- There is no guarantee that the data protection requirements are met and there may be no agreed standards in relation to the retention or backup of the data held.
- The cloud provider may store data outside the EEA and not be bound by European laws relating to the protection of personal data. This could lead to us not being in compliance with the General Data Protection Regulation.

The risks identified above mean that only University data classified as Public Data may be stored in consumer cloud services.

If a member of staff does intend to use Consumer orientated cloud storage they should read carefully the Terms and Conditions governing the use of their cloud services with particular reference to:

- Circumstances leading to account termination and potential loss of data.
- Provider's liability for negligence with respect to misuse, exposure, loss or damage of data.
- Confidentiality of data with respect to provider's data mining activities and potential resale of information for advertising, user tracking and user profiling purposes.
- Considerations about who actually owns the data and therefore has full rights over it. Some cloud providers may assert ownership of any data stored in the provider's cloud, or reserve the right to do so in future.

The financial stability of cloud providers should be considered to avoid a potential end of service with no or little notice.

Business-orientated

The use of business orientated cloud services addresses many of the risks noted above, in particular:

- The terms and conditions and service level agreement is tailored to business needs
- The organisation retains full ownership of their data
- Security of data is sometimes assured via industry standard accreditations e.g. ISO 27001
- Data retention and backup arrangements are defined
- There is no advertising built from data mining or other uses of data
- The provider's liability relating to negligence, misuse, loss or damage of data is sufficiently defined.

5. Business cloud service requirements

If a member of staff determines that they require to store Restricted, Confidential or Strictly Confidential data using cloud services for their storage requirements they must carry out the following steps prior to any use of cloud services:-

1. A Privacy Impact Assessment must be completed and submitted to dataprotection@uws.ac.uk. The Privacy Impact Assessment template can be found on the Legal Services Intranet page. On receipt of the completed Privacy Impact Assessment this will be reviewed by the Legal Services team and ITDS to determine the level of risk in using the proposed cloud based service.

2. An appropriate contract must be put in place with the provider that meets the requirements of the General Data Protection Regulation. The Legal Services team should be contacted to assist with this.

University data that is classified as Restricted, Confidential or Strictly Confidential *must not* be stored or processed using any cloud service or application unless steps 1 and 2 above have been undertaken and written approval has been received from both ITDS and Legal Services for the proposed cloud based storage.

6. Other considerations

Sharing responsibilities

Where there is a requirement to share information with others using a cloud storage service, then it is important that the staff member who enables the sharing of data does so with the following safeguards:

- Grant access only to the specific folders and files that are required to support the collaboration or information sharing. Ensure that no other folders or files are made available.
- Take care to ensure access is granted to the *correct* individuals.
- Inform all individuals involved in the collaboration or information sharing that they have a duty of care for the information provided and must honour all security requirements as well as privacy and confidentiality commitments.

Synchronising

For cloud storage services, "synchronising" files or data to a local device is not necessary, however it can provide advantages in terms of speed of access and information availability in circumstances where the user will be off-line. Synchronising information across devices requires the following safeguards:

- Devices involved in the synchronisation process must be protected from loss and unauthorised access. Mobile devices must have a "PIN" code or equivalent security enabled.
- If Restricted, Confidential or Strictly Confidential data may be involved, all synchronised copies must be protected by encryption. All mobile devices used to access Restricted, Confidential or Strictly Confidential data must be encrypted. Staff should contact the ITDS helpdesk who will help with this.
- Devices involved in the synchronisation process must be protected from malware and kept up to date with vendor supplied security patches.

7. Further information

Further details about the legal requirements under the General Data Protection Regulation can be found on the Legal Services Intranet page.

If you have any questions you can e-mail legal@uws.ac.uk