St George's, University of London
Cloud Policy

1. Policy Summary

1.1 Low Risk data may be stored or processed using a cloud service – either consumer or business-oriented. However, we recommend that you use a university supported service, such as One Drive or idrop for all types of data.

1.2 Medium and High risk data may only be stored or processed using a business-oriented cloud service, where the requirements of this policy have been met, including that the risks have been considered and addressed, the relevant areas within the University have been consulted and an appropriate contract is in place. At this time, the only general-purpose cloud storage service for which the requirements have been met is OneDrive for Business, as part of the University's Microsoft Office365 service.

1.3 Where there is a specific, currently unmet, need to sign up to, or procure any other cloud service, the requirements of section (5) must be met in full, before any data are stored or transferred.

1.4 Medium and High risk must not be stored or processed using any other cloud service or application.

1.5 Low, Medium and High risk data are as defined in the University's Information Risk Classifications.

1.6 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 SGUL premises, or stipulate specific security requirements. This may preclude use of cloud services.

2. Purpose and Scope

2.1 This Policy defines the University's position on the use of cloud services as they relate to storage or processing of University data. The Policy 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:

2.1.1 Ensure that University employees and other partners understand the University's requirements relating to the storage and guardianship of data

2.1.2 Safeguard the security, confidentiality, integrity and availability of the University's information assets.

2.1.3 Ensure compliance with national and international laws governing the storage and guardianship of data

2.1.4 Ensure compliance with contractual commitments relating to the storage and guardianship of data

2.2 The policy 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. These data may be categorised as Low, Medium and High risk - as defined in the University's Information Risk Classifications.

3. Definitions

3.1 Cloud services - are defined as services provided by an external supplier and made available to organisations, or individuals, on terms and conditions, which are defined by the external supplier. Cloud services are provided by infrastructure outside the organisation's data domain (data centres). Cloud storage services facilitate the sharing of files and make data available over a range of computers and other mobile devices, usually accessed, but not limited to web browser; mobile app; synchronisation client; drive mapping.

3.2 Cloud storage provider - examples include, but not limited to Dropbox, Box, Microsoft OneDrive, Apple iCloud, Google docs.

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

3.3.1 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.

3.4 Consumer services - where the contract is with an individual

3.4.1 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.

4. Cloud Service Risks

4.1 **Business-orientated**

4.1.1 Business orientated cloud services address many of the risks associated with the consumer versions, in particular:

- The terms and conditions and service level agreements are 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 better defined

4.1.2 As they mitigate significant risk, only business-oriented services may be used for Medium and High risk data.

4.1.3 From a corporate and legal perspective, several issues still need to be considered and addressed before deciding to use a cloud service, including:

- Data Protection legislation, governing the storage, handling and management of personal information
- Research data management, where either the organisation providing the data (e.g NHS), or the funding body have specific requirements for where data must reside e.g. in the UK, or the University
- Risks associated with automatic data synchronisation between cloud storage and University-owned or personal devices

4.2 **Consumer-orientated**

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

- There is no guarantee on data protection, retention or backup
- The cloud provider may store data outwith the UK/EU and not be bound by UK/EU laws relating to the protection of personal data.
- Individuals 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.

Because of these risks, only Low Risk data may be stored in consumer cloud services.

5. Business Cloud Service Requirements

5.1.1 The following requirements must be met, before a cloud service or application can be signed up to, or procured, for use with Medium or High risk data.

- Risks to security, including confidentiality, integrity and availability of data, and risks to privacy have been considered and addressed.
- A DPIA must be performed for the project before engaging in contract negotiations with a supplier.
- The University must have an appropriate formal contract in place with the provider organisation.

- The contract must satisfy the University's requirements for information guardianship, as well as its legal and contractual obligations.
- The following areas must be consulted, and the terms of the contract agreed with:

    - Data Protection
    - Procurement Office
    - IT Services

- The University must retain management control of the user accounts associated with cloud service subscriptions.
- The contract must address the timely recovery of lost or damaged data.
- The contract must address they timely application of critical security updates

6. Sharing Responsibilities

6.1.1 Where there is a requirement to share information with others using a cloud storage service, then it is important that individuals who enable the sharing of data do 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.

7. Data Synchronisation

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 comply with SGUL's Mobile device policy or where appropriate, BYOD policy
- If Medium or High risk data may be involved, all synchronised copies must be protected by encryption. See Encryption Policy.
- Devices involved in the synchronisation process must be protected from malware and kept up to date with vendor supplied security patches.

8. Further Information

Further details about the University's requirements and legal commitments can be found here:

Encryption Policy

Guidelines for handling Confidential Data

Research Data Management Policy

Data Protection Policy

ICO Guidance on the Use of Cloud Computing