CLOUD SERVICES

RHUL

CODE OF PRACTICE

Document Id	Cloud Services RHUL Code of Practice
Sponsor	Laura Gibbs
Author	Nigel Rata
Date	December 2014

Version Control Log

Version	Date	Change
1.0	10/10/12	Initial draft for review
1.2	26.11.12	Revised for ITUAG approval

Document Approval

Name	Approval Signature	Approval Date
ITUAG		11.12.14

Introduction

The University is currently considering its policy regarding the use of 'cloud computing services'.

Until this policy is published, cloud computing services should not be used for processing data which is:

i. Sensitive personal information as defined by the Data Protection Act (DPA) 1998;
ii. Confidential to the University or a third party;
iii. Of such criticality that functions or operations would be disrupted should it be unavailable lost or become corrupted;
iv. Valuable intellectual property of the University

This guidance document gives some background to the above.

As a member of RHUL you are responsible and liable for the data that you handle and not your line manager or Royal Holloway University of London (RHUL) itself. Any member of the University who is considering or is already using cloud storage for University information assets needs to be aware of the risks posed by using these services. This code of practice is intended to make you aware of the risks and give specific circumstances when cloud based services should not be used. It is informed by the University Information Security Policy and relevant sub policies. This guidance has been produced to help staff make decisions when considering the use of cloud based services.

RHUL IT Services provides a number of services which could be used as an alternative to taking a cloud based service. These include:

- Webdav access to y-drive from most mobile phones and tablets
- VPN for remote access to college resources
- Webmail/Activesync for access to college e-mail as well as support for all mobile device platforms.

Cloud Storage and Service providers

For the purpose of this document, cloud storage can be defined as any storage solution which stores University information assets to an online storage facility not provided by the RHUL.

Cloud-based or "capacity-based" storage is a popular solution for storing data. Cloud services are provided by large and trusted technology companies including:

Cloud Service Provider	Cloud Storage Solution
Amazon	Amazon EC2
Apple	iDisk, iCloud
Dropbox.Inc	Dropbox
Google	Google Docs, Google Apps, GDrive
Microsoft	SkyDrive, Office 365, Azure

N.B this is not an exhaustive list. Many Web 2.0 or social media applications and services often have storage capability.

Whilst these services are undoubtedly attractive, offering excellent features that are easy to use often at low cost, they bring with them a series of risks to the University and its information assets which must be considered.

Legislation and Information Assets

There are many situations where the data used by members of the University requires stringent protection which must satisfy both University regulations and government legislation. Those involved in medical research, for example, will be aware that there are obligations to protect patient confidentiality. The Information Security Policy and other policies e.g. data protection etc. provides more guidance on these matters. If there is any doubt regarding the classification of data you must seek advice from the College Secretary.

Service Providers, Contractual Agreements and Risk

All data generated as part of your duties as a member of the University belongs to the RHUL and should be managed in line with college guidance. If such data is stored on facilities provided by RHUL central IT it is protected and in compliance with the policy. Using a cloud-based storage system will put you at risk of contravening college policy or the law of the land as there are very few guarantees provided by cloud storage services. Using cloud-based storage encumbers you with a high dependency on the security of the service provider and there is often very little recourse in the event of a security breach.

This is highlighted in an extract from the Master Subscription Agreement of a cloud storage provider:

> ***"…salesforce.com shall not be responsible or liable for the deletion, correction, destruction, damage, loss or failure to store any Customer Data." 03/04/2012***
> ***http://www.salesforce.com/company/legal/agreements.jsp***

Ownership

As previously stated, all data generated in carrying out your duties belongs to the University. Using cloud storage may require you to transfer ownership of University data which you may not be eligible to do. The following extract is from the terms and conditions of the popular cloud storage provider Dropbox:

> ***"If you are using the Services on behalf of an organization, you are agreeing to these Terms for that organization and promising that you have the authority to bind that organization to these terms. In that case, "you" and "your" will refer to that organization..."***
>
> ***"You may use the Services only if you have the power to form a contract with Dropbox ...." 03/04/2012***
> ***https://www.dropbox.com/terms#terms***

Data Protection

Data protection is a complex area but its requirements apply to all members of the University. The College Secretary is the Data Controller for RHUL and may be liable for any data breach which results from the use of cloud storage. Whilst all principles of the Data Protection Act are relevant, in relation to cloud storage particular attention should be paid to Principle 8 which refers to sending personal data outside the European Economic Area.

Principle 8 states:

> ***"Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."***

Many of the popular cloud storage solutions store data on servers based in the United States. Unless they have signed up to the Safe Harbor scheme they cannot be considered to offer adequate level of protection. The following is an example from the Microsoft Azure .NET Services Platform Terms of Use:

> ***"Personal information collected through the Services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or service providers maintain facilities." 03/04 2012, http://www.microsoft.com/online/legal/?langid=en-us&docid=1***

Current debate suggests that in practice the Safe Harbor scheme offers no guarantee of compliance to the EU Data Protection Directive due to the far reaching implications of the USA Patriot Act.

Data Management

Data which has been generated as part of the carrying out your role at the University must be managed appropriately. For example, data may need to be deleted after a certain period for compliance purposes. It could be a legal requirement to demonstrate that this data has been permanently deleted and to provide supporting evidence. Clearly, this is likely to be very difficult to achieve if data has been stored in the cloud. It would also be difficult to audit exactly where the data resides, if required to do so.

Data Access

At times, data generated as part of your role may need to be accessed by colleagues or authorised members. Cloud storage solutions do not integrate with the University's authentication systems so would require all those who require access to the data to register for external accounts. If the holder of the account where the data resides is unavailable for whatever reason it may not be possible to gain timely access to the data. In some circumstances it may mean that the data cannot be accessed for long periods or may be permanently lost.

Reliability and Availability

Using cloud-based storage encumbers members with a dependency on the stability and speed of network connections. Such a connection to a cloud storage server cannot be guaranteed due to various processes from PCs/tablets/smartphones to the cloud storage servers. Depending on the features offered by the cloud storage service, it is likely that there will be a period when the data or the latest version of the data is not accessible. In the event of downtime, there is often very limited recourse.

This is highlighted both in the Amazon Web Services Customer Agreement and the Google Apps Premier Edition UK Terms and Conditions.

"[We] do not warrant that the service offerings will function as described, will be uninterrupted or error free, or free of harmful components, or that the data you store within the service offerings will be secure or not otherwise lost or damaged…" 03/04/2012 **http://aws.amazon.com/agreement/**

"Google and partners do not warrant that i) Google services will meet your requirements...ii) Google services will be uninterrupted, timely, secure or error free or reliable... iii) The results that may be obtained from the use of Google services will be accurate or reliable iv) any errors in the software will be corrected." 03/04/2012 **http://www.google.com/apps/intl/en-GB/terms/user_terms.html**

Company Viability

Regardless of the legal constraints, the long-term viability of the cloud storage company must be taken into consideration. In recent years, dozens of cloud storage companies have ceased trading after being unable to maintain commercial viability. Some of these companies have offered a means of transferring data from the cloud back to local storage or another cloud provider which entail modifying the level of complexity and varying periods of notice. As well as complete closure, other cloud storage companies have been forced to reduce their storage quotas and to introduce stricter fair use policies or increase prices in order to stay commercially viable.

Acknowledgements:

University of Liverpool and University of Leeds.