Cloud/3rd Party Services - Code of Practice

Document Summary

Document ID: Cloud/3rd Party Services Code of Practice
Status: Approved
Information Classification: Public
Document Version: 1.0 – July 2017
1. Purpose

This document states the College Cloud / 3rd Party Services - Code of Practices. It includes the roles and responsibilities of users, approved Cloud / 3rd party services and the principles of cloud / 3rd party service provider agreements.

2. Scope

The policy applies to all staff and students of the College and all other computer, network or information users authorised by the College or any department or faculty thereof.

It relates to their use of any cloud / 3rd party services for processing, storing or transmitting the College’s data.

3. Responsibilities

All: Individuals who make use of the College’s systems and information are responsible and liable for the data that they handle. Any member of the College who is considering or is already using cloud / 3rd party services for the College information assets needs to be aware of the risks posed by using these services. Responsibility for ensuring appropriate use of Cloud / 3rd party services in accordance with relevant legislation and College policies lies with the individual member of the College managing, procuring or using any Cloud / 3rd party service.

Head of Information Security: This role is responsible for ensuring that this policy is enacted and for undertaking assessment of any Cloud/3rd Party Assurance.

Information Security Team: This role is responsible for overall development of this policy, and monitoring of its effectiveness.

4. Policy:

Cloud / 3rd Party Services

Cloud service can be defined as any solution which processes, stores or transmits College information assets via an online facility not provided by the College.

Below are examples of widely used Cloud / 3rd party solutions listed but not limited to:

- Amazon – Amazon S3, AWS
- Apple – iCloud, iDisk
- Dropbox – Dropbox
- Google – Google Docs, Apps, GDrive
• Microsoft – OneDrive, Office 365, Azure
• Hosting services (Northgate)
• Events Management Services (Eventbrite) etc.

College Approved Cloud/3<sup>rd</sup> Party Service Usage

4.1. Where there is use of cloud / 3<sup>rd</sup> party services for College data, there must be a legal agreement in place between the College and the Cloud / 3<sup>rd</sup> Party Service Provider.

4.2. In some cases, it is recognised that a number of contractual agreements may be required to provide a service. Some of these will be College signed, others may require end users to hold the contractual agreement. An example of this is the use of a College managed Apple iPhone, where use is predicated on the user signing up to the iCloud service.

4.3. Users may find College approved services list in the IT Service Catalogue. Requests for the services that are not already approved and supplied by the College, should be directed to Head of Information Security via “Cloud/3<sup>rd</sup> Party Assurance Toolkit”.

4.4. Sharing credentials of any Cloud/3<sup>rd</sup> Party Service between the College managed devices and personal devices (unmanaged by the College) is not allowed unless:

   4.4.1. There is no sensitive College data
   4.4.2. Multi / Two Factor Authentication is used for either service
   4.4.3. All devices involved in this synchronising process have the same level of security with College managed devices (See Secure Build Policy)

Legislation and Data

4.5. Use of the cloud / 3<sup>rd</sup> party services must comply with applicable College policies, information security and data classification policies, regulations and government legislation, and recognised best industry practices.

4.6. Users can use College approved and supplied Cloud / 3<sup>rd</sup> party services to process, store or transmit College data. Cloud / 3<sup>rd</sup> party services should not be used to process, store or transmit “sensitive” data (See Data Management Policy) unless service contract guarantees the use of strong encryption technologies for data in transit and at rest, and contains other necessary security controls.

4.7. Use of the cloud / 3<sup>rd</sup> party services and the data processed, transmitted or
stored is subject to the same policies, regulations and government legislation that applicable to other data of the College. Anyone who is using cloud / 3rd party services must ensure that all use is consistent with associated policies, regulations and government legislation.

4.8. All data generated by College users, in carrying out their duties belong to the College. Using personal cloud storage may require persons to transfer ownership of College data which College members may not be eligible or authorised to do so. (See the Terms and Conditions of the relevant Cloud Service Provider)

4.9. Whilst all principles of the Data Protection Act and EU General Data Protection Regulation 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. (See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/, https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/)

Service Providers, Contractual Agreements and Risk

All data generated by College staff or associated members as part of their duties belongs to the College and should be managed in line with College guidance. Using a cloud / 3rd party service may create a risk of contravening College policy or the relevant legislation as there may be few guarantees provided by cloud storage services.

4.10. For all Cloud / 3rd Party services, “Cloud/3rd Party Assurance Toolkit” should be used and the use of services should be considered in terms of security and risk, data management, data access, storage, deletion and retention, auditing, reliability, and availability, viability of the Cloud / 3rd party Service Provider, and exit conditions.

4.11. Approved legal agreements with Cloud / 3rd party Services Providers must include terms about information security and cover the risk mitigation actions (if there is) that are the outcomes of assessed “Cloud / 3rd Party Assurance Toolkit” by Head of Information Security.

4.12. It is recognised that for College to participate in collaborative research it may be necessary to use cloud / 3rd party services to share with collaborators. If the College is initiating these services they should conform to the College security policies. If these services are offered by other institutions as part of the collaboration College staff should inform IT Services if sensitive data is to be stored as part of this agreement.
5. Compliance

Each part of this policy states a requirement to audit and ensure compliance with the policy. A RACI model should be applied.

**Responsible:** TSOs, Legal

**Accountable:** DPO

**Consulted:** Head of Information Security

**Informed:** All Departmental IT, Information Security, IT staff

Compliance with this policy will be checked on the following schedule.

5.1 Annual Cloud/3rd party contract review audits will be scheduled, checked and maintained.

5.2 Annual review of policy will be scheduled and reported.

5.3 Spot checks of policy compliance will be undertaken (minimum 1 per year), including review of reports and actions.

6. Policy Exclusions:

There are no formal exclusions noticed for this policy. In case of any exception request, Information Security Exception Management process should be followed.

Questions:

If you have any questions on this policy or its execution, please contact:

**IT Service Desk**

01784 444321

itservicedesk@rhul.ac.uk

itservicedesk.rhul.ac.uk

Glossary:

**Sensitive Data:** Data that must be protected from unauthorised access to safeguard the...
privacy of an individual and/or the security of the College. Sensitive data includes personal data (see Data Protection policy for details), financial data and data related to intellectual property. (See Data Management policy for definitions of data types).

Related Documents:

- IT Change control
- Vulnerability Management Policy
- Cloud/3rd Party Assurance Toolkit (Toolkit is being prepared)
- Information Security Exception Management

Acknowledgements

- University of Liverpool, University of Leeds.
### Document Control Sheet

#### Revision History

**Date of this revision:** July 2017  
**Date of next revision:** July 2018

<table>
<thead>
<tr>
<th>Revision date</th>
<th>Summary of Changes</th>
<th>Changes marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2017</td>
<td>Initial Draft – 0.1</td>
<td>No</td>
</tr>
<tr>
<td>June 2017</td>
<td>Post initial workshop comments – 0.2</td>
<td>No</td>
</tr>
<tr>
<td>June 2017</td>
<td>Post TSO Workshop – 0.3</td>
<td>No</td>
</tr>
<tr>
<td>June 2017</td>
<td>Post ISSG Workshop – 0.4</td>
<td>No</td>
</tr>
</tbody>
</table>

### Approvals

<table>
<thead>
<tr>
<th>Approvals</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratification by PRC</td>
<td>Yes</td>
</tr>
<tr>
<td>Approval by Infrastructure and Security Sub-group</td>
<td>Yes</td>
</tr>
</tbody>
</table>