Bournemouth University

IT Services

Policy Title:	**Cloud Services for Staff Policy**
Policy Reference:	**ITP0022**
IT Governance Section:	**Risk Management**
Subsection:	Information Security Mgmt
Owner:	Director of IT
Effective Date:	14/02/2012
Date of Next Review:	07/10/2016
Status:	Published

Cloud Services for Staff Policy

1. SCOPE AND PURPOSE

1.1 This policy affects the use of all 3rd party cloud and hosting services. For the purpose of this document a 'cloud service' is a service not hosted or managed by Bournemouth University (BU).

This policy exists to facilitate the use of cloud services while there are some risks associated with this type of services, this policy when viewed with the Cloud Services Guidelines aims to allow users to make good choices about the services they use.

This policy applies to all staff.

2. KEY RESPONSIBILITIES/ENFORCEMENT

2.1 Any staff who use or contracts a cloud service for University *business* is bound by this policy.

2.2 School Learning Technologists and the Learning Technology Systems team in Library and Learning Support are the primary point of contact and will guide and support staff with the use of the services for learning and teaching. These same teams will also engage IT Services when required using Service Now. They will also be responsible for agreeing the usage of Cloud Services.

2.3 The IT Service Desk will provide links to documentation and support School Learning Technologists and the Learning Technology Systems team in Library and Learning Support where necessary.

2.4 The IT Business Relationship Managers will be included should a Cloud Service employ a local client application as this will require profiling and need to be assessed using the Application Management process.

2.5 The Information Security Officer is responsible for determining and accepting exceptions from the policy upon written request.

2.6 It is the responsibility of the person requesting the use of a service to ensure the service is appropriate to their users needs and to the needs of the University detailed within this policy and accompanying guidelines.

3. LINKS TO OTHER BU DOCUMENTS/REFERENCES

3.1 This document should be read in conjunction with the Cloud Service Guidelines

3.2 Cloud Services List

3.3 Request for Cloud Service Classification

3.4 Data Protection Policy for Staff and BU Representatives

3.5 BU Non Functional Standards

Policy

4. Cloud Services

4.1 Cloud services should be considered as an option when procuring services, if appropriate solutions are available.

4.2 Careful scrutiny must be applied to the use of cloud services for *mission critical* services. Special attention must be given to the integration of BU local data sources with cloud services, e.g. Data Warehouse.

4.3 Cloud Services which are to be used for *mission critical* services must follow the BU Procurement process

4.4 Integration of cloud services with BU systems must be assessed by IT Services before the BU Procurement process is engaged

4.5 New cloud service commercial contracts must be reviewed by Procurement and Legal services. This engagement should occur as early in the process as possible to ensure enough lead time is available.

5. General Principles

5.1 The cloud service must conform to the BU Non Functional Standards e.g.AD Authentication (2008 R2+) and/or Secure LDAP

5.2 All Staff must be made aware, at the point of introduction to the cloud service, that it is not hosted by the University and that their data is stored with a third party and is subject to the terms and conditions of that service.

6. Information Security

6.1 If the cloud service requires you to *register* in order to gain access and use it you must not use your University username and password.

6.2 Staff that demonstrate informally outsourced IT facilities must not promote or approve their use for handling confidential information (and preferably should also warn against such use).

6.3 Cloud services must abide by the approved BU information security policies.

6.4 Cloud services must have appropriate data migration facilities, in and out of the service.

7. Reliability

7.1 Cloud services must have backup, recovery and retention services to meet the user's needs.

7.2 Cloud services must have Service Level Agreements to meet the user's needs.

7.3 Cloud services must have guarantees about the longevity of the service to meet the user's needs.

General

8. Definitions

8.1 Business

8.1.1 Any activity performed as part of the running of the University e.g. Learning and Teaching, Research, etc.

8.2 Register

8.2.1 When a user is required to sign up and agree to terms and conditions of a cloud based service that is not standard, recommended or approved.

8.3 Service Now

8.3.1 ServiceNow creates a single system of record for all IT processes. This system brings together IT strategy, design, transition and operation on a powerfully simple cloud platform.

8.4 Application Approval Process

8.4.1 This process reviews and validates all application requests, tests compatibility, reviews terms and conditions and assesses the risk of using an application within the University network

8.5 Mission Critical

8.5.1 A mission critical service is one that is fundamental to the delivery of a core business of the University, where there is no alternative system and the cloud service is the primary mechanism for performing the business.