University of Leicester

**POLICY FOR**
**SELECTION & USE OF CLOUD SERVICES**

| | |
|---|---|
| **Title:** | **Policy for Selection & Use of Cloud Services** |
| **Version & Status:** | **R01** |

## Policy Summary

This policy is to ensure that the University makes the best possible decisions regarding its use of Cloud based services. Cloud based services store information on remote servers, i.e. servers that don't belong to the University. These can be generic services such as Dropbox and Google Drive but also major corporate systems such as the Library Management System and Blackboard. The central principle is that we only engage with these services when we understand the implications of doing so. It is vital that the benefits, opportunities and risks have been assessed and that we have an evidential basis on which to make the decision.

The policy outlines what we should evaluate from a technology perspective when looking at a new Cloud based service. The key areas for evaluation are:

- **Data protection and information security:** The University's data is at the heart of everything we do. As such it needs to be treated with care. The University has to comply with data protection laws and we must ensure we have assessed any risks to our data from engaging with Cloud based services.
- **Interoperability and Integration with University systems:** The University benefits most from its systems when they work together. Nobody wants to enter their data many times in many systems. To make sure a new system can work securely in tandem with existing systems we need to assess how that integration will work.
- **Service provided and value for money:** It is essential - that before adopting any new services that we make sure that the University is getting the best value for money from that service.
- **Alignment with University strategy:** The University is developing a new strategy to drive its research and teaching profile into the future. With limited resources, however, we must make sure that any Cloud based systems are contributing fully to the strategy and are not taking the University in a different direction.

The policy will apply to all University staff members.

## 2. Context

Information is the key asset of the University. The University's information assets and the technology used to process, transmit and store it, needs to be appropriately and cost effectively managed, secured and governed to protect against consequences arising from the breaches of confidentiality, failures of integrity, interruption to availability and failure to comply with legal, statutory or regulatory requirements. Failure to do so may result in the University being unable to deliver its core services, while incurring significant financial costs as well as having legal implication and liability, and may also result in lasting reputational damage.

The University is governed by important regulations and working practices, particularly regarding the procurement and use of Information Technology (IT) systems and services. The governance and controls for "Formally provided, and informally available, IT facilities and services" are mature and already in place. The definition of these IT facilities and services is as defined in section 2 of *Outsourcing and Third Party Access Policy (ISP-S4)* document owned by Information Assurance Services.

The relevant regulations and governance considerations for procuring and using externally provided Information Technology (IT) systems and services are covered in number of ways:

- The Procurement Regulations (part of the University's Financial Regulation), which make specific stipulations regarding information security, particularly where procuring products and services based on Cloud Services. The Procurement Unit is the custodian of these Regulations.
- The legal, statutory and contractual aspect covered by Legal Services and the Procurement Unit. The Procurement Regulations stipulates that the University's Standard Terms and Conditions must be used for any supplier contract, unless agreed otherwise with the Procurement Unit (IT Category Manager).
- The Information Security aspects covered under the University's Information Security Policies overseen by Information Assurance Services (IAS)
- IT Services governance for alignment with technology, integration & service strategy.

## 3. Purpose

IT Services is made accountable and responsible for managing and, where appropriate, governing the technology that is used to process the University's information assets in a secure, reliable and cost effective manner, irrespective of whether they are provided by IT Services or departments; delivered using the University infrastructure or by third party outsourcing or cloud services provider.

This document covers the guidelines and governance policy related to Information Technology capability provided by the third party outsourcing or cloud services provider. (See definition of this term in section 3).

It is acknowledged that the cloud services offer number of benefits including agility, cost reduction, flexibility of scale and remote access. However there are a number of relevant policies which need to be considered carefully when using "Cloud Services" for the information assets and technology capability:

- that involves sensitive, personal or confidential information (as defined in IAS policies. See the definition in section 3)
- that involves contracts which may be above certain financial threshold
- that involves unapproved technology and/or integration considerations not aligned to University technology strategy
- where poor service quality and capability may impact on University commitments to its stakeholders

It should be noted that the Procurement Regulations, Information Assurance Services policies and standard Legal/Contractual compliance terms also covers facets of the selection and use of Cloud Services. These are administered by the respective teams and are not covered here even though there may be some technical input required for those aspects.

This document covers the IT Services technology & service considerations for the Selection and Use of Cloud Services. Further advice and guidance will be issued from time to time in recognition of the speed of change and developments in this ever changing area of technology.

## 4. Definition of Terms

The definitions of the key terms relevant to the scope of this policy document are given below.

4.1. **Confidential information:** The definition of "Confidential information" is documented and maintained in the Information Security Policy document ISP-S4. For clarity it is repeated here. Confidential information is the information which if improperly disclosed or lost could cause harm or distress to individuals, or financial loss or reputational damage to the University. This includes personal data, as defined by the Data Protection Act, and other valuable or sensitive information not in the public domain; such as the information that is commercially confidential for the University or a third party, and the information related to Intellectual Property

4.2. **Cloud Services**: In the context of this policy document 'Cloud services' is a general term for anything that involves delivering hosted technology services or cloud based products over the internet. It includes:

- The traditional definition of Cloud Services including all currently known and any new service models (IaaS – Infrastructure as a Service, PaaS – Platform as a Service, SaaS – Software as a Service), and all currently known and new deployment models (Public; Private; Community; and Hybrid cloud deployments) where there will be a formal contractual agreement between the provider and the University.
- Hosted technology or application services provided by third parties with systems hosted in either dedicated or co-located infrastructure or cloud IaaS or PaaS, or as part of shared service offerings or collaborative initiatives or any combination of the above.
- Technology elements which are part of business process outsourcing, even though the contract may be just for business processes with no explicit mention of technology.
- Cloud based services or products used to process, store or transmit University information assets, where there is a contractual agreement (often known as T & Cs or

Terms of Service to be accepted on the provider's site) between the provider and the University staff member in their individual capacity. It should be noted that this specific arrangement is already covered in the Information Security Policy ISP-S4 *"Outsourcing and Third Party Access Policy (ISP-S4)"* and those guidelines and controls will not be repeated in this document.

4.3. **Service User/Procurer**: The University staff member, student supervisor, collaborator or the authorised agent who is involved in or responsible for procuring, selecting and using the Cloud Services being used to process or manage University information assets.

## 5. Roles and Responsibility

5.1. IT Services will be responsible for creating and updating this policy. The Information and Communications Technology Committee (ICTC) or equivalent governance group will be responsible for approving this policy.

5.2. IT Services will be responsible for governance and implementation of this policy in conjunction with associated stakeholder in this area, viz. Procurement Unit, IAS and Legal services.

5.3. The Service User/Procurer commissioning and planning the use of the cloud services is responsible for ensuring full compliance with this policy. Failure to comply with any university policy may lead to disciplinary action.

5.4. The final decision on non-compliance with this policy will rest with the Director of IT Services.

5.5. Any approval to proceed despite non-compliance must be obtained from the ICTC or the Registrar & Secretary as appropriate who will take into account the concerns raised by IT Services and who will accept the relevant risks or may undertake to address and resource the management of any risks and issues raised.

## 6. Policy Details

6.1. This policy applies to the procurement, selection and use of all type of cloud services irrespective of the financial contract value for such service provision (including free, freemium, any type of subscription model, annual charges or part of a multiyear contract).

6.2. This policy supplements the regulation and policy directives covered by the *Procurement Regulations* and the Information Security policies, especially the "*Outsourcing and Third Party Access Policy (ISP-S4)".* Hence aspects covered in those regulations and policies will not be repeated here.

6.3. The Service User/Procurer must contact IT Services via their IT business partner in the initial instance to ensure compliance with Cloud Service Policy when the works, services or goods to be procured are to be provided by Cloud Services as defined above, irrespective of the financial contract value of such services.

6.4. Where relevant IT Services will consider and request risk assessment by Information Assurance Services to determine the applicable ISPs and risk level for the proposed service to help determine the appropriate technical controls expected from the service. The approach and detail of such risk assessment is covered in the Outsourcing and Third Party Access Policy (ISP-S4).

6.5. The Information risk assessment is to be carried out on the advice and guidance of IAS when the Cloud Service provider will process, transmit or store University information asset that is of sensitive, personal or confidential nature.

6.6. IT Services will assess and consider whether the proposed service is compatible with the University's broader technology strategy.

6.7. IT Services will assess and consider whether the proposed service can be provided by existing services or technology capability portfolio.

6.8. IT Services will assess and consider whether the proposed service is acceptable, covering the following areas (but not limited to this list):

- Technical standards, in particular compliance with Authentication, Authorization, Integration, web domain and end user devices standards
- Relevant non-functional requirements, in particular technical security, availability, resilience, scalability, interoperability and technology life span and viability etc.
- Service management and support aspects, especially if the Service is going to be used by a large number of University users.
- Technical aspects of Business Continuity and Disaster Recovery
- Technical considerations for end of service scenarios (Exit strategy)
- The requirement for management information and reporting

6.9. IT Services may also liaise with Procurement unit, Legal Services and IAS to ensure that appropriate account is taken of technical and service aspects in the procurement exercise and ultimate contract, including the specification, tender evaluation criteria, terms and conditions and service level agreement. It should be noted that as stipulated within the Procurement Regulations, the University's Standard Terms and Conditions must be used for any supplier contract, unless agreed otherwise with the Procurement Unit (IT Category Manager)].

6.10. IT Services may also assess and consider whether the proposed service is providing good value for money in the wider context.

6.11. IT Services may also assess and advise on the service quality offered by the cloud service provider

6.12. Where the due consideration and assessment by IT Services concludes that a proposed Cloud Service does not comply with the policy based on the criteria specified in this document, or if IT Services is of the opinion that it is not offering good value for money or the service quality is deemed not fit for purpose, then either an alternative service must be found or approval to proceed must be obtained from the ICTC or the Registrar & Secretary, as appropriate, who will take into account the conclusions of the assessment by IT Services.