



University College Dublin Cloud Computing Self Evaluation Guidelines

Updated: 15 October 2017

Contents

Introduction	3
Cloud Computing – Defined	3
New challenges with Cloud Computing	3
Purpose of these guidelines	4
Who does these guidelines apply to?	4
What data and information do these guidelines apply to?	4
Data and Information classification	5
Legal and policy basis	6
Criteria for all cloud services	7
Procedure to procure, evaluate, use cloud service	8
Appendix A – Cloud Computing Checklist	10
A.1 Introduction	10
A.2 Checklist instructions	10
A.3 Checklist roadmap	10
A.4 UCD stakeholder and institutional requirements	11
A.5. Application Security Considerations	12
A.6 Support arrangements	19
A.7 Exit strategy	20
A.8 Document checklist	20
Appendix B – General Advice on Contractual Issues	21
B.1 Contracts	21
B.2 Transfer of personal data outside of the EEA	21
B.3 Service level agreement	21
B.4 Agreeing the right terms with a cloud provider	22

Introduction

This document sets out the College's Guidelines for evaluating cloud computing services, also known as cloud computing, cloud services or cloud.

Cloud Computing – Defined

Cloud computing is a method of delivering Information and Communication Technology (ICT) services where the customer pays to use, rather than necessarily own, the resources. These services are typically provided by third parties using Internet technologies. The widely accepted definition of cloud computing provided by the US Government's National Institute of Standards and Technology (NIST), is adopted for convenience noting that the Irish Department of Public Expenditure and Reform has also developed a similar definition. At present there are four widely accepted service delivery models:

- Infrastructure as a Service (IaaS);
- Software as a Service (SaaS);
- Platform as a Service (PaaS);
- Network as a Service (NaaS).

Cloud services are provided via four deployment models:

- Private cloud – where services are provided by an internal provider, i.e. IT Services "[Cloudedu](#)";
- Public cloud – where services are provided by third parties, i.e. external companies or entities, over the public Internet;
- Community cloud – where services are provided by external company(s) or entity(s) for a specific community of users with common interests;
- Hybrid cloud – where services are provided partly by an internal provider in a private cloud and partly provided by an external company(s) or entity(s) in the public or community cloud.

Cloud services can provide a significant range of benefits to individuals and organisations including increased solution choice and flexibility, faster time to solution, and reduced total cost of ownership. However, the cloud also presents new challenges.

New challenges with Cloud Computing

The processes involved in procuring and evaluating cloud services can be complex and subject to legal, ethical and policy compliance requirements. These requirements must be evaluated and met prior to signing up to and using cloud services. This is essential to ensure that personal, sensitive and confidential business data and information owned, controlled, or processed by the College, its staff, students and its agents is adequately protected at all times. The service must be selected to ensure that the data and information is secure and that an adequate backup and recovery plan is in place to ensure that data and information

can be retrieved to meet business needs. For more critical systems, the service should be built with high availability, again to meet business needs. In short, any IT service holding and processing such data and information must be fit for purpose and meet business requirements.

The purchasing of ICT goods and services, including cloud services, is subject to contract law and EU procurement directives. The cumulative total contract value of a procured service from a given company over a fixed time period, generally one year, is subject to differing public procurement thresholds and approaches. Multiple individuals or agents carrying out discrete procurement of the same service, while acting on behalf of the College, may inadvertently, and against College policy, purchase contracts with a cumulative value that exceeds procurement thresholds, breaching legislation.

Historically, the steps involved in procuring and evaluating ICT services have rested with a multifunctional team of trained professionals in IT Services, IT security, procurement (Finance), and law (UCD Legal office). With the consumerisation of IT, the availability of low cost or free cloud services, such as software as a service, and the ease of Internet access, there is an increased likelihood that College staff or agents will bypass these professionals and the appropriate control procedures and put themselves and the College at risk by procuring and / or using inappropriate cloud services.

Purpose of these guidelines

The guidelines are a statement of the College's commitment to ensuring that all its legal, ethical and policy compliance requirements are met in the procurement, evaluation and use of cloud services.

Who does these guidelines apply to?

This guidelines apply to all staff and students and to all agents or organisations acting for, or on behalf of, the College in the evaluation, procurement or use of cloud services.

What data and information do these guidelines apply to?

These guidelines apply to all personal data, sensitive personal data and confidential business data and information (to include legal documents not already in the public domain) defined as:

- 'personal data' means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller;
- 'sensitive personal data' means personal data as to:
 - the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
 - whether the data subject is a member of a trade union,
 - the physical or mental health or condition or sexual life of the data subject,

- the commission or alleged commission of any offence by the data subject, or
- any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;
- ‘Confidential business data and information’ is data and information which concerns or relates to the trade secrets, processes, operations, style of works, sales, purchases, transfers, inventories, or amount or source of any income, profits, losses, or expenditures of the College, or other organization, or other information of commercial value, the disclosure of which is likely to have the effect of either impairing the College's ability to obtain such information as is necessary to perform its statutory functions, or causing substantial harm to the competitive position of the College, or other organization from which the information was obtained, unless such information is already in the public domain. Such data and information will simply be referred to as confidential business data and information.

Data and Information classification

Personal data, sensitive personal data, and College’s confidential business data and information is classified as shown in Table 1:

Table 1: Data and Information Classification

Data / Information Classification		Description	Examples	Handling
Non-confidential	Public	Such data is available for anyone to see, and is often made available to the public via the College web site.	Term dates, dates of College closures. Staff names and contact details. School names and addresses.	Access to this data is not usually restricted, i.e. a username and password are not required to access this data
	University Internal	Such data is generally available to all staff and students in College.	General meeting minutes. Day to day activities and communications	Access is usually restricted to members of College staff.
Confidential	Restricted	Personal data. Confidential business data and information This is data that is usually	Documents subject to Data Protection Legislation. Confidential memos. Confidential	Access to this data is restricted to the people that are entitled to use it, but generally this will be a large

		not made available to all staff, and which could result in legal action, reputational damage or financial loss.	information related to Research or Funding.	number of staff and the data is not as confidential or sensitive as the critical data described above.
	Critical	Sensitive personal data. Confidential business data and information inappropriate use of this information could result in legal action, financial loss and severe reputational damage to the College.	Information relating to the mental and physical health of individuals. Data subject to a confidentiality clause. Financial data such as bank account numbers or payment cards. Biometric identification data. Upcoming Exam papers	Access to such data is tightly controlled, with only a few individual users being entitled to see or use the data. Critical data is generally stored in purpose built applications, often in an encrypted format, even within internal secure systems.

Legal and policy basis

The procurement, evaluation and use of cloud services must adhere to the legislation in force at the time. Particular attention must be paid to:

- Copyright and Related Rights Acts 2000, 2004 and 2007;
- GDPR 2016 – Enforced May 25th 2018;
- Data Protection Acts 1988 and 2003;
- Freedom of Information Act 1997 and 2003;
- Contract Law;
- EU Public Procurement Directives;
- The Child Trafficking and Pornography Acts 1998 and 2004;
- Defamation Act 2009;
- Prohibition of Incitement to Hatred Act 1989.

All information held in the cloud is considered to be a record held by the College and therefore may be the subject of a Data Protection or Freedom of Information access request.

The procurement, evaluation and use of cloud services must adhere to the College policies in force at the time. Particular attention must be paid to the following policies:

- Acceptable Use Policy;
- Data Protection;
- Freedom of Information;
- Procurement;
- Intellectual Property;
- Ethics;
- Good Research Practice;
- Accessible Information;
- Use of the College's trademarks;
- Dignity and Respect;

Criteria for all cloud services

All Cloud Services must:

- Be fit for the purpose they are designed to support;
- Comply with all relevant Irish and European Legislation.
 - [The Universities Act 1997](#)
 - [The Higher Education Authority Act 1971](#)
 - [The Comptroller and Auditor General Amendment Act 1993](#)
 - [Copyright and Related Rights Acts 2000, 2004, 2007](#)
 - [GDPR Regulations 2018](#)
 - [Data Protection Acts 1998 and 2003](#)
 - [Safety, Health and Welfare at Work Act 2005](#)
 - [Freedom of Information Acts 1997 and 2003](#)
 - [Official Languages Act 2003](#)
 - [Ethics in Public Office Acts 1995](#)
 - [Standards in Public Office Act 2001](#)
 - [Equality Act 2004](#)
 - [Equal Status Act 2000](#)
 - [Disability Act 2005](#)
 - [The Child Trafficking and Pornography Act 1998 and 2004](#)
 - [Defamation Act 2009](#)
 - [The Civil Partnership and Certain Rights and Obligations of Cohabitants Act 2010](#)
 - [The Ombudsman \(Amendment\) Act 2012](#)
- Comply with all existing College Policies.
 - [Academic Secretariat Policies](#)
 - [Data Protection Policy](#)
- Respect the intellectual property rights of others and not breach copyright when using cloud services.
- Meet College Accessibility Requirements.
- Comply with the relevant professional [ethics and with the College's ethical principles](#). Where ethical issues arise in the use of cloud services, the guidance of School and Faculty Ethics Committees must be sought in advance of the use of the service;

- Comply with the College's Policy on Good Research Practice: Where necessary and appropriate, the guidance of the College's Research Committee and the Research Ethics Policy Group must be sought before using a cloud service for research purposes.

Procedure to procure, evaluate, use cloud service

All staff and students and all agents or organisations acting for, or on behalf of, the College in the procurement or evaluation of cloud services, or planning on using cloud services to store or process data or information obtained through their work or interaction with the College must ensure that the following steps are adhered to:

- The cloud service proposed is suitable for the type of data and information which is to be stored or processed in the cloud as defined in Table 1 (above) and Table 2 (below):

Table 2: Data and Information / Cloud Service Deployment Model Compatibility Matrix

Data / Information classification	Cloud Service Deployment Model		
	Internally hosted / private cloud with appropriate security controls and management running applications designed for the data that they store	Public / Community / Hybrid Cloud with formal privacy and security policies such as ISO/IEC27001	Public Cloud without a guarantee of security or privacy
Critical	Yes	No	No
Restricted	Yes	Yes	No
University Internal	Yes	Yes	No
Public	Yes	Yes	Yes

- Approval to use data or information: Where a cloud service is proposed to host College data or information, appropriate written sign off must be received from the data or information owner / controller and from the Head of School or Administrative unit or their designee. This written sign off should be retained;
- Approval that data or information can be hosted in the cloud: Following approval from 2., and evaluation against 1., where a cloud service is proposed to host personal data, personal sensitive data or confidential business data and information, then before entering into a cloud service agreement the proposed cloud service must be reviewed, tested as appropriate, and approved to ensure that confidential data can be processed and stored securely. These guidelines and the checklist provided in Appendix A must be followed and adhered to;

- For a new cloud service: contact procurement at the start for procurement advice and/or information on existing cloud agreements in place;
- The College places great emphasis on the need for integration (all systems should be able to talk to each other) and interoperability (systems should be able to work on and be moved to different environments) of systems. These requirements must be considered and documented;
- IT Services must be contacted at evaluation stage for advice where data from a cloud service is required to integrate with an internal College system. Where integration is required, all College policies, procedures and project prioritisation must be adhered to;
- Backup / Retention / Business Continuity / Disaster Recovery: The service must be selected to ensure that the data and information is secure at all times and that an adequate backup and recovery plan is in place to ensure that data and information can be retrieve in a timely manner to meet business ness. For more critical systems, the service must be built with high availability, with a business continuity and disaster recovery plan that fits business needs. IT Services must be contacted for advice and sign off in advance where a cloud services is being considered to provide a business critical IT system;
- An appropriate formal contract must be put in place with the cloud service provider (see Appendix B for guidance), it is generally not appropriate to simply accept the third parties generic terms and conditions. College Procurement must be consulted and provide written sign off in advance to ensure that appropriate contract law, procurement legislation and College policies are adhered to;
- For a new cloud service: The individual or agent must ensure that all criteria for cloud services have been met and submit their checklist (Appendix A) to the UCD Legal and UCD Procurement so the service can be evaluated;
- Approval must be obtained from the UCD Legal Affairs and UCD procurement before a new service can be purchased or used for the first time;
- Approval must be obtained from the College Solicitor before using an approved College cloud service if the service has not been approved for the classification of data and information under consideration.

Appendix A – Cloud Computing Checklist

A.1 Introduction

This checklist is intended to assist those in College who are considering using cloud computer services for all or part of their official College work. Where difficulties are experienced completing this checklist advice should be sought from IT Services – clearly indicating where there is uncertainty with the answer.

As requirements can vary considerably this document should be regarded as a non-exhaustive checklist that highlights to sponsors the likely implications of using cloud computing.

Please note that this document cannot anticipate every issue that might arise in every project nor is it intended to take the place of a properly resourced project proposal or plan.

A.2 Checklist instructions

- The answers to the questions should be in the first instance compiled by the College department(s) in MS Word.
- Questions should be answered as concisely and as fully as possible in the document.
- The input of vendors should be incorporated as needed. Inclusion of vendor promotional materials or references should be avoided or kept to the minimum.
- If the question is not considered relevant or cannot be answered by the department please state this in the table below.
- Where answers are very detailed, place a reference (e.g. NOTE 1) in the table below and then full reply placed at the end of the document.
- Where the information in an answer is considered confidential, please preface the answer with [CONFIDENTIAL].

A.3 Checklist roadmap

- Completed self-evaluation checklist and associated documents should be submitted to IT Services Security Office “Security@ucd.ie” for advice.
- An external security company may be required to review the security of cloud services. The purchaser of the cloud service will be responsible for any costs associated with an external cloud review.
- Some projects may require input from the other College departments such as UCD Legal, Data Protection, Procurement office, Bursars office, Library, Research Ethics and others. If required, please contact the relevant department for additional advice.

A.4 UCD stakeholder and institutional requirements

This section deals with the service and the implications of its use for the College. This section should be completed by UCD.

No.	Questions	Answer
1.	Which College departments are stakeholders in the proposed system?	
2.	List the names of College sponsors for the system. These would normally be Heads of Department, Schools or senior members of staff.	
3.	Name of University project manager	
4.	Name of departmental contact person (usually person collating the information in this document)	
5.	What business need(s) does this system fulfil? Please append if available.	
6.	Is this a new system or replacing an existing system? If replacing an existing system, please specify the name of the existing system.	
7.	Have detailed user requirements been documented and agreed by the stakeholders? Please append if available.	
8.	What groups of people will be using this system? e.g. postgraduate students, staff members etc.	
9.	What would be the impact to University if the service was unavailable?	
10.	Is this a public or private cloud service? A public service is offered without modification by the vendor. A private service is where the vendor modifies the service to meet specific University requirements.	PUBLIC/PRIVATE
11.	Does the application contain personally identifiable information? If Yes, please specify what PII data will be stored in the system.	
12.	Can data generated by the vendor product be supplied to other University	

	systems that might need it e.g. Student system? This is to identify potential “silo” systems.	
13.	How long in years is it projected that the service will be used?	
14.	<p>Please list independent reference sites and contacts using this service.</p> <ul style="list-style-type: none"> ○ Site name and address: ○ Year started usage: ○ Site contract name and email: <p>Has these sites been contacted by UCD?</p>	
15.	Will the system need data from core University systems such as Student Information System, Personnel, Finance or Research Support Systems? The permission of the relevant University data owner will be needed to use data of this type.	List of Data Owners

A.5. Application Security Considerations

This section outlines issues and security considerations in relation to the vendor offering the service. This section should be completed by the application vendor/cloud service provider.

No.	Question	Answers
Vendor Detail		
1.	Vendor Name	
2.	Product Name	
3.	Product Description	
4.	When was the vendor company established?	
5.	What year did the vendor start to supply this service?	
6.	Vendor contact name	
7.	Vendor contact title	
8.	Vendor contact email	

9.	Vendor contact phone number	
10.	Which country or jurisdiction is the vendor based in.	
11.	How many higher education, commercial customers and government customers do you serve in Ireland and Europe? If applicable, please provide a list of higher education customers.	
12.	Describe the structure and size of the vendors IT Security Office and overall information security staff.	
13.	Describe the structure and size of the vendor Software and System Development teams	

Documentation \ Compliance

14.	Has the Vendor undergone an ISAE 3402 or SSAE 16 audit?	
15.	Has the vendor completed the Cloud Security Alliance (CSA) self-assessment or CAIQ?	
16.	Does the vendor conform to industry standard security frameworks? (e.g. ISO 27001, NIST Special Publication 800-53, etc.)	
17.	Please supply current copies of vendors IT security policy and supporting documentation.	
18.	Please supply current copies of the application privacy policies.	

Application Compatibility

19.	List any client operating systems or versions that the vendor product cannot work on?	
20.	List any client web browsers or versions that the vendor's product cannot work on?	

Architecture

21.	Is the service a single-tenant or multi-tenant environment?	
22.	Can access to the application be restricted to the University's network?	
23.	Please provide overall system and/or application architecture diagrams	

	including a full description of the data communications architecture for all components of the system?	
24.	Is the institution's data physically and logically separated from that of other customers?	
25.	Specify what controls that are in place to secure the vendor remote environment and connection to institution data. _ role based _ Citrix _ multi-factor _ Other	

Authentication, Authorization, and Accounting

26.	Describe how application user security administration is performed?	
27.	Can user access be customized to allow read-only access, update access, or no-access to specific types of records, record attributes, components, or functions?	
28.	Can the application enforce the University minimum password/passphrase complexity requirements of 8 characters containing at least 1 uppercase letter, 1 lowercase letter and 1 number?	
29.	Select the types of authentication, including standards-based single-sign-on, that are supported by the web-based interface? _ SSO _ InCommon _ Shibboleth _ Other	
30.	Does the system (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP, Shibboleth) in place of local authentication?	
31.	Does the system support Multi-Factor authentication? If so, please specify supported MFA services.	

32.	Does the application support password changes at a frequency no greater than 180 days?	
33.	Does the application require a user to set their own password after an administrator reset or on first use of the account?	
34.	Does the application lock-out an account after a number of failed login attempts?	
35.	Does the application automatically lock or log-out an account after a period of inactivity?	
36.	Does the application logs record access including specific user, date/time of access, and originating IP of device?	
37.	Does the system provide data input validation and error messages?	
38.	Does the system have the capability to log security/authorization changes as well as user and administrator security (physical or electronic) events (e.g., login failures, access denied, changes accepted), and all requirements necessary to implement logging and monitoring on the system. Include information about SIEM/log collector usage.	

Data Security

39.	Does the application contain personally identifiable information? If Yes, please specify what PII data will be stored in the system.	
40.	Please outline the application backup procedures. e.g. The frequency of backups, off site locations, how many copies are retained, how long are backups retained, etc.	
41.	Is data encrypted in transport? e.g. TLS, SFTP, SSH. Please provide details.	
42.	Is data encrypted at rest? e.g. Database encryption, disk encryption, backup encryption, etc. Please provide details.	

43.	Will the vendor allow other organizations access to the data stored on the cloud system?	
44.	Are any sub-contractors or other vendors involved in the provision of the service? Please provide details.	
45.	Will the University retain ownership of the data at all times?	
46.	If the vendor ceases trading who would own the data?	
47.	Who controls access to the data within the vendor's organization?	
48.	Are vendor employees allowed to take home customer data in any form?	

Data Protection

49.	Does the service comply with E.U General Data Protection regulations (GDPR)?	
50.	Which jurisdiction will the data reside, including backups? e.g. European Economic Area "EEA", USA, etc. If data resides outside of the EEA, please specify what data protection arrangements are in place to ensure the data is protected in line with EU data protection regulations 1998, 2003 and GDPR. e.g. EU/US Privacy Shield, modal contracts, etc.	
51.	What procedures does the cloud provider have in the event of a data breach? The University's Data Protection Officer must be informed of both a suspected and actual breach within 24 hours of the breach being discovered.	
52.	Does the contractual and financial terms protect the University from a data breach by the cloud provider?	
53.	How would the vendor address:	

	<ul style="list-style-type: none"> ○ Persons who wish to view their data under Data Protection, Freedom of Information or other legislation? ○ Persons who wishes to amend or remove their data (Right to be forgotten) 	
--	---	--

Data Centre Security

54.	List all datacentres including cities and countries where the institution's data will be stored. Does your company own these data centres?	
55.	Does the vendor own the physical data centre where University data will reside? If so, do these servers reside in a co-located data centre?	
56.	Does the hosting provider have a SOC 2 Type 2 report available?	
57.	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	

Disaster Recovery & Business Continuity

58.	What would be the impact to University if the service was unavailable?	
59.	Please outline the disaster recovery procedure in the case that a data centre, servers, or other infrastructure get damaged or destroyed.	
60.	Are any disaster recovery locations outside the EEA? If so, please provide the locations.	
61.	Are all components of the Disaster Recovery Plan reviewed at least annually and updated as needed to reflect changes?	
62.	Describe the Business Continuity Plan?	
63.	Is there a documented communication plan in your BCP for impacted clients?	
64.	Does your organization have an alternative business site or a	

	contracted Business Recovery provider?	
65.	Does your organization conduct an annual test of relocating to this alternate site for business recovery purposes?	
Application Security Controls		
66.	Has the service been securely developed and configured to be available directly from the internet?	
67.	Is the system utilizing a web application firewall (WAF) and / or a stateful packet inspection (SPI) firewall?	
68.	Is the service monitored for intrusions on a 24x7x365 basis?	
69.	Describe or provide a reference to any other safeguards or intrusion prevention controls used to monitor or prevent attacks?	
70.	Will the University be immediately alerted of intrusions or malicious events?	
71.	Has the applications undergone an independent third party penetration test or audit in the last year? If so, please provide details of the external company who carried out the test and include a high-level overview of the results.	
72.	Are your applications and infrastructure scanned for vulnerabilities on a regular basis?	
73.	What was the date of your last application/Infrastructure vulnerability assessment? (dd/mm/yyyy)	
74.	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.	
75.	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).	

76.	Describe or provide a reference to any other safeguards, security controls or intrusion prevention controls used to monitor or prevent attacks?	
-----	---	--

A.6 Support arrangements

No.	Issue	Further details	Refer to
1.		Request suppliers to provide detailed breakdown of the 5 year support and maintenance cost.	
2.		Request suppliers to provide detailed breakdown of the 5 year support and maintenance cost.	
3.		Is there a roadmap for the service/application in terms of product updates/support and testing?	
4.		How is support provided by the company to your environment e.g. Helpdesk, remote management, is admin rights required?	
5.		Can you provide sample service agreement detailing maintenance and support services including scheduled maintenance plans, uptime, and response times?	
6.		Please indicate if any other third party manages any part of the support? If the solution is a multi-vendor solution please provide details of how support calls are handled.	
7.		Please describe your support organisation, account management, including locations and total number of support staff.	

A.7 Exit strategy

This section clarifies what happens when the cloud service ends.

No.	Issue	Further details	Refer to
8.	Notice	What notice must the College give to terminate the service?	Vendor contract
9.		What notice does the vendor have to give to terminate the service?	Vendor contract
10.	Data	How and in what format will the College's data be returned after termination?	Vendor contract
11.		Will the returned data be in a format that can be migrated to another future system?	Vendor
12.		Will the vendor be allowed keep copies of the data after the termination?	Vendor contract
13.		Will the vendor be able to demonstrate that all copies of the data will be destroyed, including backups.	Vendor contract

A.8 Document checklist

These documents are likely to be needed. The variety of applications means a definitive list is difficult to compile.

Document name	Question #
Fully completed checklist (this document)	
Agreed user requirements	
Vendor IT security policy	
Application Privacy policy	
Vendor Business Continuity Plan	
Independent IT security audit	
Vendor Service Level Agreement	

Appendix B – General Advice on Contractual Issues

The details provided below are for information purposes only and does not constitute legal advice. For specific legal advice please contact the Solicitor's Office.

B.1 Contracts

If you propose to use a cloud service, you must have a contract in place with the third party that covers the provision of the service. Matters to be included in the contract are:

- Data protection;
- Intellectual property rights;
- Freedom of information obligations;
- Legal compliance;
- Law enforcement and loss of control;
- Licensing;
- Confidentiality of data;
- Monitoring by the cloud provider;
- Law and jurisdiction;
- Data retention schedules;
- Subcontracting;
- Acceptable use policy;
- Warranties;
- Indemnities;
- Exclusions and limitations of liability;
- Change of service by the cloud provider;
- Termination.

B.2 Transfer of personal data outside of the EEA

If data is likely to be stored outside the EEA, you might be in breach of the Data Protection Act unless there are adequate security measures in place for personal data. Compliance may be achieved if [EU approved contract clauses](#) are used with a cloud provider. Alternatively, if using a US based cloud provider, ensuring that they are signed up to the EU/US Privacy Shield provisions will be necessary.

Further details on your obligations when considering sending personal data outside the European Economic Area are available on the European Commissions website - http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm

B.3 Service level agreement

A service level agreement (SLA) describes the service that the third party will provide, the performance targets (e.g. service availability, problem resolution, support, incident resolution, change control, security, etc) and mechanisms for compensating the College if the SLA targets are not met. You must ensure that the contract for cloud services includes an SLA that meets your business needs.

B.4 Agreeing the right terms with a cloud provider

The cloud provider contract on offer must be examined in detail and favourable and constructive terms negotiated with the cloud provider to ensure that they are appropriate to the work that the College carries out.

Cloud providers are likely to offer the same (standard) service to multiple users so the College may have to change its applications and processes to match what is offered.

The key to the negotiation at this point is to ensure that enough control is maintained in house in order to minimise the legal risks while still taking advantage of the opportunities that cloud computing can bring.

Some Questions to clarify with the Cloud provider:

- What “Information Security Standards” does the provider adhere to?
- Does the cloud provider use third parties to evaluate its own security risks?
- What identity and access management architecture is in place?
- How will the cloud provider accommodate the obligations that the institution has with regard to data protection and data retention schedules?
- Are there clear penalties in the contract for data loss or breach of security and privacy?
- Can the cloud provider give assurances that information can be taken down without delay from websites or other accessible locations on the instruction of the service provider or IT Service management team?
- What planned responses are in place should a service failure occur?
- Can the cloud provider’s facilities be inspected by the College’s representatives?
- Is data portability part of the service that is provided?
- Where encryption of data is required is the cloud provider able to facilitate this requirement?