COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH
Ollscoil Átha Cliath

TRINITY COLLEGE DUBLIN
The University of Dublin

Cloud Computing Policy and Guidelines

Release: 1.51

1. Introduction

This document sets out the College's policy for the use of cloud computing services, also known as cloud computing, cloud services or cloud.

1.1. 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[1] 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[2]. 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. IS Services;
- 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.

1.2. 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.

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] http://per.gov.ie/wp-content/uploads/Cloud-Computing-Strategy.pdf

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 IS Services, IT security, procurement (Finance), and law (Secretary's 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.

2. Purpose of this policy

This policy is 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.

2.1. Who does this policy apply to?

This policy applies 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.

2.2. What data and information does this policy apply to?

This policy applies 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[3]' 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[4]' means personal data as to:
  a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
  b) whether the data subject is a member of a trade union,
  c) the physical or mental health or condition or sexual life of the data subject,
  d) the commission or alleged commission of any offence by the data subject, or
  e) 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

[3] As defined in Section 1(1) of the Data Protection Acts 1988 and 2003

[4] As defined in Section 1(1) of the Data Protection Acts 1988 and 2003

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.

2.3. 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: Trinity College Dublin 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 not made available to all staff, and which could result in legal action, reputational damage or financial loss.	Documents subject to Data Protection Legislation. Confidential memos. Confidential information related to Research or Funding.	Access to this data is restricted to the people that are entitled to use it, but generally this will be a large 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. Biometric identification data.	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.

3. 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;
- 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:

- Data Protection;
- Freedom of Information;
- Procurement;
- Intellectual Property;
- Ethics;
- Good Research Practice;
- Accessible Information;
- Use of the College's trademarks;
- IT and Network Code of Conduct;
- College Web;
- Dignity and Respect;
- Social Networking and Social Media Policy.

4. Criteria for all cloud services

All Cloud Services must:

1. Be fit for the purpose they are designed to support;
2. Comply with all relevant Irish and European Legislation. See https://www.tcd.ie/about/legislation/ for information on applicable legislation and compliance.
3. Comply with all existing College Policies. A comprehensive list of current policies is available at: http://www.tcd.ie/about/policies/;
4. Comply with Irish and European data protection legislation;
5. Respect the intellectual property rights of others and not breach copyright when using cloud services. See https://www.tcd.ie/Secretary/compliance/ for guidance;
6. Meet College Accessibility Requirements. See http://www.tcd.ie/accessibility/ for further information;

7. 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;
8. Comply with the College's Policy on Good Research Practice: https://www.tcd.ie/media/tcd/about/policies/pdfs/Policy-on-Good-Research-Practice_1.1.pdf. 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.

5. 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:

1. 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 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

2. 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;
3. 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. This policy and the checklist provided in Appendix A must be followed and adhered to;
4. For a new cloud service: contact procurement at the start for procurement advice and/or information on existing cloud agreements in place;
5. 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;

6. IS 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;
7. 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. IS 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;
8. 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;
9. 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 Secretary to the College and the Director of IS Service so the service can be evaluated;
10. Approval must be obtained from the Secretary to the College and the Director of IS Services or their appointed nominees before a new service can be purchased or used for the first time;
11. Approval must be obtained from the Secretary to the College and the Director of IS Services or their appointed nominees before using an approved College cloud service if the service has not been approved for the classification of data and information under consideration.

If the service is a new cloud service, and passes all the above steps, then the Secretary to the College and the Director of IS Services will designated the service a College approved cloud service, for the given classification of data and information. IS Services will publish a list of all College approved cloud services.

6. Policy compliance and handling of policy breaches

1. The Secretary to the College and the Director of IS Services, or their appointed nominees, reserve the right to refuse College staff, students or agents permission to use any new cloud service or to enforce the discontinued use of an existing cloud service if it is deemed by them to be unsuitable for any reason;
2. The Secretary to the College and the Director of IS Services must be notified in writing of all cloud services procured and in use by staff, students or agents of the College that holds College data and information or that has been procured on behalf of the College;
3. In exception circumstance, having due regard for the appropriate legislation and policies, the Secretary to the College and the Director of IS Services may authorise derogations from this policy;
4. Where it is alleged that a breach of policy has occurred the matter should be reported by the complainant to the Secretary to the College. Thereafter, in consultation with Staff Office and the Director of IS Services, as appropriate, an investigation will be established to ascertain the facts following the existing procedures agreed with the various staff and student representative bodies. Depending on the outcome of the investigation it may be necessary to establish a formal disciplinary hearing. Any such disciplinary hearing will be conducted in accordance with the relevant College disciplinary procedure.

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 IS 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 checklists and associated documents should be submitted to IS Services Programme Management Office in the normal way and will be considered in accordance with PMO procedures.
- The submission will be acknowledged by email and a Remedy tracking case will be created. The case will initially be managed by the IS Services Programme Management office.
- The checklist will be assessed and a member of IS Services may be in contact to progress the matter.
- Further clarification may be needed on certain points. These will be referred to the contact person named below.
- Some projects will require input from the other College departments such as Secretary's office, Financial Services Division, Library and others. It will be assumed that the disclosure of parts of the checklist to persons in these departments can proceed unless the section is marked otherwise.

A.4 Stakeholder and institutional requirements

This section deals with the service and the implications of its use for the College.

No.	Questions	Reply
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 or senior staff.	
3.	Name of departmental project manager	
4.	Name of departmental contact person (usually person collating the information in this document)	
5.	List the name of the vendor(s) and their contact details. Any sub-contractors should also be listed.	
6.	Outside the vendors, please list any parties external to College involved in the solution.	
7.	What business need(s) does this system fulfil?	
8.	Have the detailed user requirements been documented and agreed by the stakeholders? Please append if available.	
9.	What groups of people will be using this system? E.g. postgraduate students, staff members etc.	
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 College requirements.	PUBLIC/PRIVATE
11.	Can data generated by the vendor product be supplied to other College systems that might need it? This is to identify potential "silo" systems.	
12.	How long in years is it projected that the service will be used?	
13.	What is the budget for this project and where is it sourced from?	
14.	Is the budget provided sufficient for the entire procurement and life time of the service?	

A.5 Vendor considerations

This section outlines issues to be considered in relation to the vendor offering the service.

No.	Query	Reply
15.	When was the vendor company established?	
16.	What year did the vendor start to supply this service?	
17.	Can they supply a banker's reference? Please append.	
18.	Are their audited company accounts available? Please append.	
19.	Please list independent reference sites and contacts using this service. • Site name and address: • Year started usage: • Site contract name and email: • Has this site been contacted by TCD:	

No.	Issue	Further details	Refer to
20.	Jurisdiction	Which country or jurisdiction is the vendor based in.	Vendor
21.		Which jurisdiction will the data reside?	Vendor
22.	Site security	Does the vendor have a current independently compiled security audit of their site?	Vendor
23.		How often are security audits conducted and by whom?	Vendor
24.	Levels of Service	Does the vendor provide a Service Level Agreement that sets targets for the services it offers?	Vendor
25.		Is there a documented and enforceable means of complaints resolution?	Vendor
26.		How does the vendor charge for its services? E.g. annual charge, numbers of students etc.	Vendor
27.		If the service level needs to be scaled up or down how is this to be accommodated in the cost of the service?	System sponsor
28.		Has the College secured future price protection for this service?	System sponsor
29.	Continuity of service	Does the vendor have adequate documented arrangements for dealing with computer disasters and ensuring a continuity of service to College?	Vendor
30.		What would be the impact to College if the service was unavailable?	System sponsor
31.	Compatibility	List any operating systems or versions that the vendor product cannot work on.	Vendor
32.		List any web browsers or versions that the vendor's product cannot work on.	

A.6 Data issues

This section deals with College data and the implications of its use. System sponsors will need to consider if the cloud solution justifies the risk of processing data offsite and the possible costs security audits. For sensitive data a College hosted system may offer cost savings in the long term.

No.	Issue	Further details	Refer to
33.	Data ownership and safety	Will the system need data from core College systems such as Student Administration, Personnel or Research Support Systems? The permission of the relevant College data owner will be needed to use data of this type.	Data owner(s)

No.	Issue	Further details	Refer to
34.		Will the vendor allow other organizations access to the data stored on the cloud system?	Vendor
35.		Will the contract allow the vendor disclose any of the data to others without the College's permission.	Vendor
36.		Are sub-contractors or other vendors involved in the provision of the service?	Vendor
37.		Will the College retain ownership of the data?	Vendor and system sponsor
38.		How long will data reside on the system?	Vendor
39.		If the vendor ceases trading who would own the data?	Vendor and system sponsor
40.		Who controls access to the data within the vendor's organization?	Vendor
41.	Data sensitivity	Is the system dealing with information that must be kept confidential? Data Protection and other legislation apply to cloud computing services. Examples might include :- • Names or contact details of College students or staff • Academic grades • Research data or results • College financial information etc.	System sponsor
42.		What steps will the vendor take to safeguard sensitive information?	Vendor
43.		The vendor should supply current copies of their IT security policy and supporting documentation.	Vendor.
44.		How are backups of data secured by the vendor?	Vendor
45.	Data required	What data will be required? Most vendors supply a list of the data fields they require. This should be given to the data owner.	Vendor
46.		Is data encryption required? What data encryption mechanism does the vendor provide?	Vendor
47.		How are users to be authenticated for the service? Does the cloud service support the Shibboleth / SAML 2.0 or ADFS protocol to facilitate connection to TCD's Federated Access authentication system?	Vendor
48.	Data Protection and other legislation	How would the vendor address:- • Persons who wish to view their data under Data Protection or other legislation? • Persons who wish to amend or remove their data?	Vendor
49.	Transparency to service users	How will those using the new service be made aware that their data is been processed off-site and possibly their data is being stored off-site?	

A.7 Payments details

Many cloud systems generate a need for collection of payments for services. This section need only be filled if financial transactions are to be processed through the cloud service.

#	Issue	Further details	Refer to
50.		Does the application need to accept payments for College Services? Write 'Nil' if no financial transactions are involved.	College sponsor
51.		What is the anticipated annual total amount of payments using this service?	
52.		What is the anticipated annual number of transactions?	College sponsor
53.		How does the vendor facilitate payments?	Vendor
54.		What guarantees are there that the payment mechanism is secure?	Vendor
55.		How will the financial transactions be accounted to the Treasurer's Office?	College Sponsor/Treasurers Office

A.8 Support arrangements

No.	Issue	Further details	Refer to
56.		Request suppliers to provide detailed breakdown of the 5 year support and maintenance cost.	
57.		Is there a roadmap for the service/application in terms of product updates/support and testing?	
58.		How is support provided by the company to your environment e.g. remote management, is admin rights required?	
59.		Can you provide sample service agreement detailing maintenance and support services including scheduled maintenance plans, uptime, and response times?	
60.		Please provide details of your service billing and charging methods?	
61.		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.	
62.		Please describe your support organisation, account management, including locations and total number of support staff.	

A.9 Exit strategy

This section clarifies what happens when the cloud service ends.

No.	Issue	Further details	Refer to
63.	Notice	What notice must the College give to terminate the service?	Vendor contract
64.		What notice does the vendor have to give to terminate the service?	Vendor contract
65.	Data	How and in what format will the College's data be returned after termination?	Vendor contract
66.		Will the returned data be in a format that can be migrated to another future system?	Vendor
67.		Will the vendor be allowed keep copies of the data after the termination?	Vendor contract

A.10 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)	n/a
Agreed user requirements	
Vendor IT security policy	
List of required data fields	
Bankers reference	
Audited company accounts	
Vendor Business Continuity Plan	
Independent IT security audit	
Vendor Service Level Agreement	
Vendor contract	

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 Secretary'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 terms are used with a cloud provider. Alternatively, if using a US based cloud provider, ensuring that they are signed up to the Safe Harbour provisions will be necessary. You can check this on the USA Trade Information Centre - Export.gov website at - https://www.ftc.gov/business-guidance/privacy-security/data-privacy-framework.

Further details on your obligations when considering sending personal data outside the European Economic Area are available at https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations.

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, 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 IT director?
- 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?