Cloud Computing Guidance

Table of Contents

Cloud Computing Guidance.. 1

Rationale Underpinning this Cloud Computing Guidance...1

Cloud Computing Highly Recommended Guidelines... 3

Section A: EU General Data Protection Regulation (GDPR) Considerations.................3

Section B: IT Security Considerations...4

Section C: Identity and Access Management considerations......................................6

Section D: Procurement and Contractual Obligations...6

Section E: General Administration & Support...6

Additional Support.. 7

Version History... 7

Rationale Underpinning this Cloud Computing Guidance

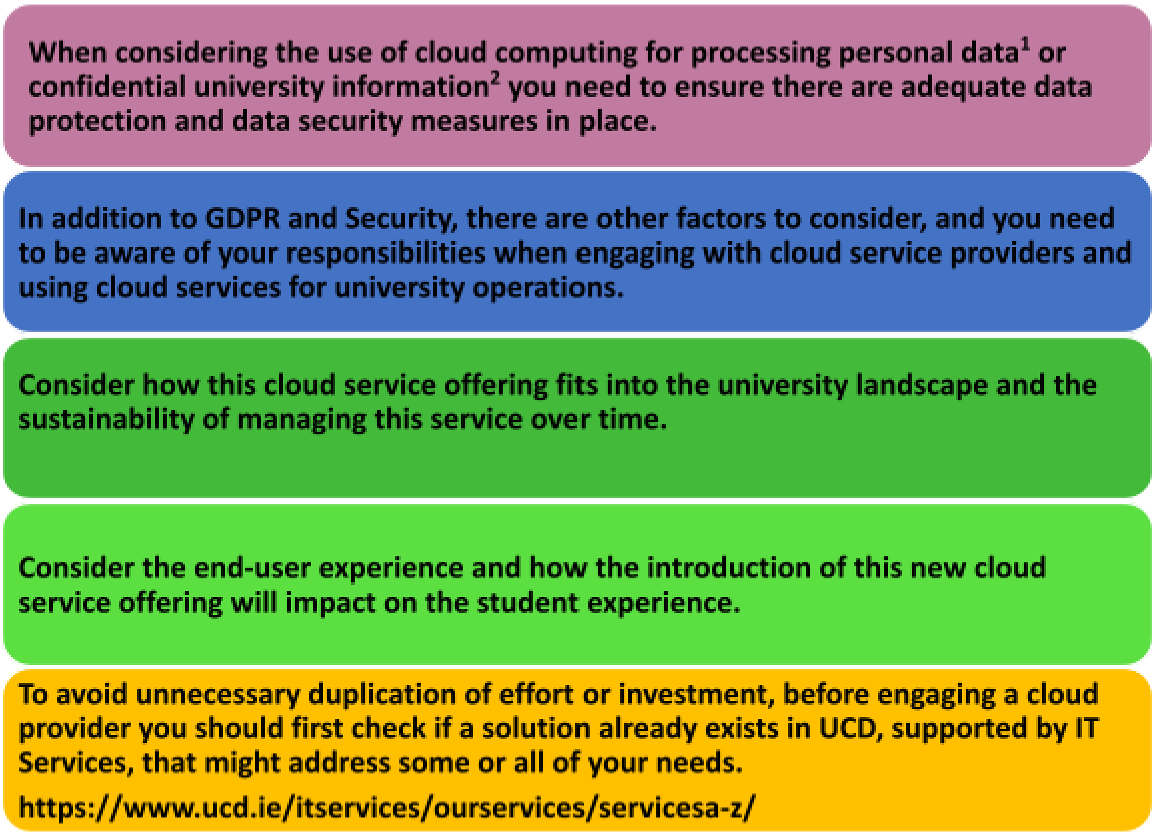
Rising to the Future UCD Strategy (2020-'24) includes *'Transforming Through Digital Technology' as one of the core themes permeating everything we do and identifies 'Implement advanced systems and services to support our operations'* as a key enabler.

"*In each case we will ensure that the appropriate digital systems are in place to simplify and reduce the need for staff time to be absorbed in routine tasks… making the campus a model of working in the digital age*." (p.32)

In responding to this enabler, faculty and staff are increasingly engaging with cloud service offerings, including 'cloud storage', allowing documents, photos, videos, and other files to be uploaded to and stored on a remote server, to enable sharing or remote access, or to act as a backup copy. There is also a growing trend towards deploying cloud solutions managed locally within a school or unit outside the remit of IT Services.

In order to ensure the best practice is consistently followed, IT Services have identified a number of core principles for engaging with cloud services that should be adhered to.

Core Principles Underpinning Alignment of Cloud Computing Services with UCD's Strategy



When considering the use of cloud computing for processing personal data[1] or confidential university information[2] you need to ensure there are adequate data protection and data security measures in place.

In addition to GDPR and Security, there are other factors to consider, and you need to be aware of your responsibilities when engaging with cloud service providers and using cloud services for university operations.

Consider how this cloud service offering fits into the university landscape and the sustainability of managing this service over time.

Consider the end-user experience and how the introduction of this new cloud service offering will impact on the student experience.

To avoid unnecessary duplication of effort or investment, before engaging a cloud provider you should first check if a solution already exists in UCD, supported by IT Services, that might address some or all of your needs.

https://www.ucd.ie/itservices/ourservices/servicesa-z/

*[1] **Personal Data** consists of any information concerning or relating to a living person who is either identified or identifiable. An individual could be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (such as an IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual*

*[2] **Confidential University Information** consists of information which, if disclosed or made publicly available could damage commercial or financial interests, privacy, employability, could cause damage or distress to individuals, cause the University to not meet its legal obligations e.g. GDPR or PCI compliance or damage the University's reputation.*

Cloud Computing Highly Recommended Guidelines

Section A: EU General Data Protection Regulation (GDPR) Considerations

Where personal information is involved, you have a legal obligation under GDPR. Where UCD is the data controller, and you act on behalf of UCD, you must remain in control of the personal data when subcontracting the processing to a cloud provider. A key element of control is to ensure the security of the data.

Controllers (yourself on behalf of UCD and the cloud service providers) also need to be transparent about the processing of personal data. In many cases this will require a 'Privacy Notice/Statement' to be drawn up to inform users of the data relating to them that is collected and used in connection with the service, as well as the uses (including disclosures to third parties) that is made of such data.

There is also a legal requirement for a written contract with the cloud service provider. When processing personal data you have a legal obligation to comply with these and other GDPR regulations.

- Consider if the solution will be recording or accessing personal or health related information. If so, ensure compliance with GDPR regulations, in particular Article 32 which refers to the security of processing; your data controller responsibilities; and the responsibilities of the data processor(s) who mostly will be a third party.

- Ensure that all personal data will remain within the EEA so that they benefit from maximum privacy protection under EU law. Where you cannot ensure that all personal data will remain within the EEA you need to complete an 'International Transfer of Data Agreement' with the vendor.

- Complete a Data Protection Impact Assessment (DPIA) where relevant. For further details on GDPR please see: https://www.ucd.ie/gdpr/guidanceresources/

Also review the Guidance for Engaging Cloud Service Providers published by the Irish Data Protection Commission.

Section B: IT Security Considerations

If *personal* or *confidential* university information is involved or its availability impacts critical operations of the university then the security of the solution is a priority.

Before considering a cloud computing service or engaging a cloud service provider, you should be satisfied with the reputation of the cloud provider and that their security standards are sufficient and appropriate.

	Considerations
1.	The cloud service provider should have **recognised information security accreditations** which demonstrate a structured and organised approach to managing information security. When assessing cloud service you should seek evidence of **independent certifications** against recognized information security frameworks such as ISO/IEC-27001, SOC2, Cloud Security Alliance CCM, etc.
2.	The cloud provider undertakes **independent security assessments** of the cloud service, infrastructure and policies at regular intervals or after any significant change such as major upgrades, a migration to a new hosting provider, etc. Security assessments of the service should include: ● Penetration and Network Security Assessments (ideally every 12 months) ● Vulnerability scans (ideally every month) ● Security Policy Reviews (ideally every 12 months) ● User Access control assessments (after upgrades)
3.	UCD's **data** is **physically or logically separated** from other customers' data.
4.	All personal or confidential information must be **encrypted while in transit** (e.g. TLS, SSH, SFTP) **and at rest** (e.g. Full disk encryption, database encryption, backup encryption, etc.).
5.	**Technical and procedural security measures** have been implemented to prevent, detect and respond to cyber and insider threats. Look for evidence that the following security measures are in place: ● Secure development practices. ● Patch management procedures. ● Intrusion prevention measures including network, host and web application firewalls. ● Intrusion detection solutions that actively monitor (24x7x365) the cloud service for threats such as malware, suspicious user behaviour, malicious network traffic, server security events, etc. ● All security activity is logged and retained for auditing purposes.
6.	Procedures need to be in place in the event of a **data breach of personal or confidential university information**, including an incident response plan that has been

	agreed between UCD and the cloud service provider, so that data subjects are not unnecessarily put at risk.
7.	**The ability to respond and restore access to University** information in a timely manner in the event of a physical or technical incident. Look for evidence that: ● Backups are retained for at least 1 month, backups are verified and restores tested at least every 12 months. ● Incident response, communication and a disaster recovery plan are reviewed and tested annually.
8.	The cloud provider has a documented **shared responsibility model** that clearly describes UCD's responsibilities for ensuring the security of data, applications and infrastructure in the cloud.
9.	If the service requires people to log on, and personal or confidential university information is involved, which might be put at risk, or if the service is being rolled out to a significant cohort of students, faculty, or staff, then IT Services recommends that the service is **integrated with UCD's Single Sign On (SSO) service**. *To support UCD SSO, the cloud solution will need to support Shibboleth/SAML authentication protocols.*
10.	All cloud service passwords must be protected in line with UCD **Password Protection policy**. In addition ● Where UCD's SSO is not being used and authentication is managed locally by the cloud provider, users must not under any circumstances reuse their UCD Connect Password or a variation of it. The account setup screen and password reset screens should include text to remind users in this regard. ● The University does not support third party authentication services such as login with Facebook, LinkedIn, etc. ● All locally stored passwords within the service must be protected using irreversible hashing functions such as BCRYPT, PBKDF2 or similar irreversible hashing function.
11.	If the cloud service stores or processes sensitive personally identifiable information, an **external security assessment** of the service should be organized by UCD's application owner prior to going live with the solution. Please contact IT Services IT Partners for information on external security reviews. For solutions outside of IT Services systems portfolio, the cost of external reviews must be funded by the school or unit engaging with the cloud service.
12.	The cloud service provider provides a means to securely **erase and return all University data when a contract terminates**. The contract with the cloud service provider must stipulate how University data will either be returned and/or securely erased, including data held on backups when the contract terminates.

For further Security relate information see:
https://www.ucd.ie/itservices/ourservices/security/

Section C: Identity and Access Management considerations

13.	**A "Joiner, movers & Leavers" process is in place to create and remove accounts from the service as employees leave UCD or move to new positions**. Leaving access to University systems unmanaged may have data protection implications, particularly if accounts have access to other users' data.
14.	The cloud solution must support granular or **role based access** controls which can be configured to ensure that users permissions are based on their job function. UCD Application administrators must ensure that all user accounts are set up with the **'minimum access rights and permissions'** that are required for application users to complete their job function.
15.	**Privileges accounts** such as accounts with administrator permissions **must take extra steps to protect their account**, such as enabling Multi-Factor Authentication or set strong, unique passwords with a minimum of 15 characters.

Section D: Procurement and Contractual Obligations

16.	Ensure that **public sector procurement rules are adhered** to, details available at: https://www.ucd.ie/procure/
17.	If personal data is to be store on the cloud, procurement specifications need to include **Data Protection by Design**[3] **and Default**[4] **GDPR** (Article 25)
18.	Ensure that all necessary **legal and support documentation** is in place including any contract and service level agreements (SLAs) needed. Where personal information is involved a contract must be in place with the cloud provider in line with GDPR regulations (controller processor agreement) details available at: https://www.ucd.ie/corpsec/functions.html
19.	Consider if cover for loss of data, data breaches, cyber attacks, etc. are a concern and if so that there is **adequate insurance cover in place**, details available at: https://www.ucd.ie/sirc/insurance

Section E: General Administration & Support

20.	**Ensure that the responsibilities and tasks associated with supporting a cloud service are clear and well documented**, not just for the initial deployment but for the lifecycle of the solution. The role of an application owner (i.e your responsibilities) typically include: ● Managing user accounts and permissions. ● System administration. ● Vendor management. ● Monitoring and responding to security events.

	● Ensuring all supporting documentation is maintained. ● Training and supporting users of the solution. ● Data breach management and timely breach reporting.
21.	Ensure that an adequate **support agreement** (e.g. 9-5, 24x7) is in place prior to deployment, with agreed service level agreements (SLAs) and clear escalation processes.
22.	Ensure that any **internal support processes** are in place prior to deployment so that you have contact details for the cloud provider should any issues arise with the service.
23.	Ensure that the solution has a **backup facility to support your business needs**. You should also consider if Disaster Recovery (DR) or Business Continuity (BC) is adequately covered, and that all university information can be accessed as and when required.

[3] **Data Protection by design** means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

[4] **Data Protection by default** means that the user service settings (e.g. no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all.

Additional Support

Having reviewed the information and links above, if you need further assistance contact IT Services Partnership Team: itpartners@ucd.ie

Version History

Name	Version	Date	Reason for Change
IT Services	**v1.8.5**	**August 2021**	**Approved by ITLG**
IT Services	**v1.8.6**	**June 2023**	**Editorial amendments layout**
IT Services	**v1.8.7**	**Nov 2023**	**Alignment with digital solutions technical controls.**