Cloud Computing Guidance V1.8.5

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 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 Guidance V1.8.5

Cloud Computing Highly Recommended Guidelines

Section A: EU General Data Protection Regulation (GDPR)

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 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

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.

Key security factors include:

1. The cloud service provider should ideally have industry standard information security accreditations such as ISO-27001. The system architecture should be scanned for vulnerabilities at regular intervals and an independent security audit / penetration test should be completed every 12 months.

2. In the absence of the above, the cloud service provider should be able to provide evidence that ensures the ongoing confidentiality, integrity, availability and resilience of the service, evidence of their security development standards and evidence of technical security features incorporated into the platform such as a web application firewall, stateful network firewall, intrusion detection and prevention controls, malware protection, key activity is logged and retained for auditing purposes, etc.

3. 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.). Locally stored passwords must be protected using an irreversible hashing function such as BCRYPT.
4. UCD’s data must either be physically or logically separated from other customers data.

5. 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.

6. The ability to restore availability and access to University information in a timely manner in the event of a physical or technical incident. The backup procedure should retain copies of University data for at least 1 month, the vendor should have an incident response plan, communication procedure and a disaster recovery procedure, which are reviewed and tested at regular intervals.

7. A means to securely either delete or 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.

8. If the service requires people to log on, and personal or confidential university information is involved, which might be put at risk, or the service is being rolled out to a significant cohort of students, faculty, or staff, then IT Services recommends that the service be integrated with UCD's Single Sign On (SSO) service. This would allow users to securely login using their UCD IT Account.

9. The cloud solution will need to support Shibboleth/SAML authentication protocols to integrate with UCD’s SSO.

10. The University does not support third party authentication services such as login with Facebook, LinkedIn, etc.

11. Where UCD’s SSO is not being used and authentication is managed locally by the cloud provider, users should use a Unique password and **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.

12. Locally stored passwords within the service must be protected using irreversible hashing functions such as BCRYPY, PBKDF2 or similar irreversible hashing function. This is for security purposes to prevent data breaches where third party solutions hold local copies of passwords, their system is compromised, and malicious actors use the stolen credentials to access university systems.

13. Where there is a possibility that personal or confidential information is put at risk, the solution must enforce good password management protocols, meaning that a strong password that meets UCD’s Password Protection Policy, and preferably the service should support Multi-Factor Authentication (MFA) (also referred to as 2nd Factor Authentication (2FA)).

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

Section C: User Accounts and Managing Access

14. It is recommended that a process is in place to create and remove UCD accounts from the service as employees leave the University. Leaving access to University systems unmanaged may have data protection implications, particularly if accounts have access to other users’ data.

15. User accounts should be setup with the ‘minimum access rights and permissions’. This means they should get only as limited access to the system as necessary to carry out their role.

16. Users with administration permissions must take extra steps to protect their account, such as enabling Multi-Factor Authentication or setting password with a minimum of 15 characters.

Section D: Procurement and Contractual Obligations

17. Ensure that public sector procurement rules are adhered to, details available at: https://www.ucd.ie/procure/

18. 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)

19. Ensure that all necessary legal documentation is in place including any 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

20. 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

21. Ensure that general roles and responsibilities are clear, not just for the initial deployment but on an ongoing basis. To consider things like general vendor management & support, ongoing service configuration, data breach management and timely breach reporting, day to day administration, ongoing training requirements, etc.

22. 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.

23. 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.

24. Ensure that the solution has a backup facility to support your business need. 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.

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

[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.*