Cloud Computing Policy

1. Context

Trinity College Dublin, the University of Dublin, hereafter referred to as the University, uses cloud computing technology to process and store University data and to provide digital services to employees, students, visitors, and the public.

Cloud computing presents the University with the potential to avail of scalable, flexible, innovative and cost-efficient computing services to facilitate University operations. All new University systems should be developed to take advantage of the opportunities presented by cloud deployment models where possible, in line with a cloud first approach.

The cloud computing policy provides comprehensive guidance to all relevant University personnel acting for, or on behalf of, the University in the procurement, evaluation, implementation, configuration, use, support of cloud services. To enable them to ensure that cloud-based solutions align with business objectives, regulatory requirements and technology based best practices.

The policy provides a due-diligence and risk-based approach to cloud system selection, deployment and management.

2. Purpose

The cloud computing policy is required to ensure that all cloud services in use in the University have been procured appropriately and are suitable for the type of data and processing involved, that they are maintained securely, and that the University is in compliance with all relevant legislation.

This is essential to ensure that personal data as well as other general confidential and important University data owned, controlled, processed by, or otherwise the responsibility of the University, its employees, students and its agents is processed only in systems which are appropriate for the data, adequately maintained and secured, and is protected at all times.

3. Scope

Trinity College Dublin

This policy applies to all employees and students and to all agents or organisations acting for, or on behalf of, the Univeristy in the evaluation, procurement, implementation, mangement or use of cloud computing services.

University Data

This policy applies to all University data including but not limited to personal data, special categories of personal data and confidential University data.

Cloud Deployment Method
This policy applies to all types of cloud deployment; Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a Service (Saas).

This policy applies to all types of cloud systems including public cloud, private cloud and hybrid cloud.

Cloud Procurement/Use of non fee paying services
This policy applies both to cloud systems which require fees and/or licences and to those which do not charge a fee for use.

4. Principles

Cloud computing services are generally suitable for any information or system subject to appropriate considerations and risk assessment.

It is important to note that while University faculties, schools, professional service areas and commercial units may delegate the delivery of a service to a cloud service provider or a third-party intermediary, they cannot delegate their overall responsibility or accountability for that service and the safety of the data stored within it.

Responsibility for compliance, safety and the ongoing operational effectiveness of a cloud computing service is a shared responsibility between the University, the service vendor and system users as outlined in the contract, service level agreement and acceptable use policies.

The School, Unit or Individual who is responsible for procuring or selecting the cloud computing service is responsible for ensuring that the cloud system adheres to this policy at all times over the life of the service until such time as it is safely decommissioned.

5. Definitions

Term	Definition
Cloud computing	The delivery of computing services—such as servers, storage, databases, networking, software, processing, applications, analytics, and artificial intelligence via the internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. With cloud computing instead of owning and maintaining physical data centres or servers, organizations like Trinity College can access these services on-demand from a cloud provider like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP).
Infrastructure as a Service (IaaS)	A cloud computing model that provides virtualized computing resources over the internet (cloud). It offers basic IT infrastructure—for example virtual machines, storage, and networking. Examples of this include Amazon EC2, Microsoft Azure virtual machines etc.
Platform as a Service (PaaS)	A cloud computing model that provides a ready-to-use platform which can be used to build, run, and manage applications—but without having to manage the underlying infrastructure (like servers, storage, or networking).

	Examples of this include AWS Elastic Beanstalk Microsoft Azure App Services etc.
Software as a Service (SaaS)	A cloud computing model where a fully functional software application is provided over the internet. End users can access the software via a web browser or app, without needing to install, maintain, or manage the underlying infrastructure or platform. Examples of this include Microsoft365, Google Workspace etc.
Public Cloud	A public cloud infrastructure designed and configured for open and shared use by the general public which exists on the premises of the cloud provider. Public cloud providers offer standard, repeatable services at scale and on-demand. Hyperscale providers operate on a global basis with regional deployment.
Private Cloud	A cloud computing environment dedicated exclusively to a single organization. Unlike public clouds—where resources are shared among multiple users -\. a private cloud provides exclusive access to computing resources such as servers, storage, and networking. For example the IT Services provided cloud.
Personal Data	Any information relating to an identified or identifiable person who can be identified, directly or indirectly, by reference to an identifier such as name, image, identification number, location data or online identifier.
Special Categories of Personal Data	Data revealing an individual's racial or ethnic origin,political opinions, religious beliefs or philosophical beliefs, data relating to trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health and data concerning an individual's sex life or sexual orientation.
Confidential University data	Non-public data and information pertaining to the Univeristy whose unauthorized disclosure could cause harm to the University. This data is protected by internal policies, contracts, or legal regulations. Examples include, student and staff personal data, commercial data, research data.
Business-critical priority activity	The services provided by Trinity College to students, researchers, academic, administrative & technical staff, visitors, and other interested parties* to which priority must be given following an incident in order to mitigate impacts. **Interested parties – a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.*
General Data protection Regulation (GDPR)	The General Data Protection Regulation (GDPR) is the data protection law enacted by the European Union (EU) that governs how organizations collect, process, store, and share personal data of individuals within the EU and the European Economic Area (EEA). The GDPR came into effect in May 2018, and applies to any organization regardless of physical location which handles the personal data of EU/EEA residents.
Data Protection Impact Assessment (DPIA)	A process required under the General Data Protection Regulation (GDPR) when a data processing activity is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is a legal requirement under Article 35 of the GDPR. Note you must conduct a DPIA if your project involves; new technologies, systematic monitoring of individuals (e.g., CCTV in public spaces), large-scale processing of sensitive data (e.g., health, biometrics, political beliefs), automated decision-making that significantly affects individuals.

Cyber Security Assessment:	A structured evaluation of an organization or an ICT systems' digital infrastructure, policies, and practices. It is conducted in order to identify vulnerabilities, assess risks, and determine the effectiveness of existing security controls Conducting cyber security assessments on cloud systems provides the University with assurance that the University data held in the system will be secure and protected from cyber threats.
Artificial Intelligence (AI)	Refers to the technological simulation of human-like intelligence in machines. AI is powered by algorithms, data processing, and models that enable it to recognize patterns, make decisions, and improve over time.
University Digital Asset Register	A register maintained by the University which lists all significant computing systems in use in the University along with relevant information about the system such as the name of the supplier and the name of the University area of personnel responsible for the system.
Relevant Irish and European legislation	Is defined within the scope of this policy as including but not limited to the legislation listed below: • The General Data Protection Regulation (EU) 2016/679 (GDPR) • Data Protection Act 2018 • Regulation on Artificial Intelligence (AI Act) • The eprivacy regulations 2011 S.I. No.336 of 2011 • Data Protection Act 2018 (Section 36(2)) (Health Research Regulations) • Intellectual Property Miscellaneous Provisions Act (2014) • Copyright and Related Rights Act (2000) • S.I. No. 59/2012 - European Union (Copyright and Related Rights) Regulations 2012. • Electronic Commerce Act (2000) • ECommerce Directive (2000/31/EC) • Regulations entitled European Communities (Directive 2000/31/EC) Regulations 2003 (S.I. No. 68 of 2003) • Freedom Of Information Act 2014

6. Cloud Policy Statement

Before entering into a contract, deploying or using a new cloud computing system or service, all employees, students, agents or organisations acting on behalf of the University or who are planning to use cloud computing services to store or process data or information obtained through their work or interaction with the University must:

6.1 Ensure that they have the **appropriate approval** from the relevant data steward, accountable head of school or professional unit to use, collect or store University data in the proposed cloud computing system.

6.2 Ensure that they are in compliance with all applicable University policies and procedures on the **procurement** of cloud computing systems. The most up-to-date information and advice on procurement can be obtained from the Financial Services Division (FSD).

6.3 Ensure that they are aware of and have adhered to all **legal and compliance** requirements including ensuring that all contracts have been appropriately reviewed and that all other **relevant Irish and European legislation** has been considered. Advice and sign off should be sought from the Secretary's office.

6.4 Ensure that the processing of the data within the cloud system is in compliance with the **General Data Protection Regulation (GDPR)**. A data protection impact assessment (DPIA) may be required depending on the nature and scale of the data processing proposed. Advice and sign off should be sought from the University Data Protection Office.

6.5 Ensure that they have identified any components of the cloud computing system that are using **Artificial Intelligence (AI).** AI components of a system may be subject to additional compliance requirements under the Regulation on Artificial Intelligence (AI Act). There is also an obligation to make system users aware of such components and their role in the processing of their data.

6.6 Ensure that the system complies with best practice **cyber security standards**. Cloud system vendors should be vetted and required to evidence compliance with a suitable cyber security certification such as ISO27001. Cloud systems should use appropriate encryption mechanisms to protect data and vendors should provide evidence of ongoing security testing of the system or service. A Cyber Security Assessment will usually be required, dependent on the scale and nature of the data processing involved, before implementation and periodically thereafter. Advice and sign off should be sought from IT Services.

6.7 Ensure that they have considered the need for **Integration** with other University systems, IT Services must be contacted at the cloud computing service evaluation stage for approval where data from a cloud service is required to integrate with another University IT System or requires a transfer of University data from other IT systems.

6.8 Ensure that an adequate **backup and recovery plan** is in place to ensure that data and information can be retrieved in a timely manner to meet business needs. For critical systems, the service must be built with high availability and with a business continuity and disaster recovery plan that fits business needs. Business Continuity must be contacted for advice in advance of deployment where a cloud service/hosting is being considered to provide an IT system for a business-critical activity.

6.9 Ensure that **incident response and breach notification procedures** are adequately defined in the contract and/or service level agreement. Advice and guidance on compliance with cyber security and compliance requirements can be obtained from the Data Protection Office and IT Services.

6.10 Ensure that all users of the system will receive adequate **instruction, guidance and training** on the appropriate and safe access to and use of the cloud system and that these are documented for users in the form of an acceptable usage policy.

6.11 Ensure that they assign a named University employee as the cloud **business system administrator** who will be accountable for overseeing any day-to-day system or account administration that may be necessary for the operation of the system throughout its life. Guidance on best practice business system administration can be obtained from IT Services.

6.12 Ensure that the cloud system will comply with **accessibility requirements t**o ensure that all staff and students have equitable access to information and information systems. Advice and sign off should be sought from the Trinity disAbility office.

6.13 Ensure compliance with all relevant policies and guidelines related to **good research practice**. The guidance of the University's Research Committee and the Research Ethics Policy Group should be sought when selecting a cloud service for research purposes.

6.14 Ensure the purpose, use, processing and data use of any proposed new cloud computing system or service is aligned with the University Strategic Plan, Data Management policies and Technology Strategy. Advice and sign off should be sought from the Data Analytics & Strategic Initiatives Unit and IT Services.

6.15 Ensure compliance with all existing **University policies**. A comprehensive list of current policies is available on the University policies website.

6.16 Ensure that when the system is **decommissioned** at the end of the life of the cloud computing system that all University data is securely removed from the cloud system. A written statement should be obtained to that effect from the cloud computing system vendor.

7. Policy Owner

Policy Owner
The Cloud Policy is owned by the Secretary to the College and the Director of IT Services.

Breach of Policy
Where it is alleged that a breach of policy has occurred the breach should be reported to the Secretary to the College and/or the Director of IT Services.

Right of Refusal
The Secretary to the College and the Director of IT Services, or their appointed nominees, reserve the right to refuse 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.

8. Responsibility and Implementation

Faculty Deans/Heads of Schools/Professional Services Areas/Commercial Units
Faculty Deans/ heads of schools/professional services areas and commercial units are responsible for ensuring that all cloud systems specifically procured/selected/used in their faculty, academic schools, or research centres; and professional service areas or commercial units are in compliance with the cloud computing policy.

Heads of Schools/Professional Services Areas/Commercial Units
Heads of schools/professional services areas/commercial units are responsible via their representative on the Federated digital, data and cyber security group to ensure that all cloud systems procured/selected/used in their areas are listed and maintained on the University digital asset register.

Cloud Business System Administrator
The cloud business system administrator **i**s responsible for overseeing any day-to-day system or account administration that may be necessary for the safe and efficient operation of the cloud computing system. This may include but is not limited to; account administration and user access reviews, creating/removing user accounts, timely notification and responding to identified or suspected vulnerabilities, incidents and breaches, as well as conducting regular vendor meetings to ensure that cloud vendors are in compliance with their contractual arrangements and agreed service level agreements.

Federated Digital, Data and Cyber Security Group Members
Is responsible for promoting awareness of the policy among faculties, Schools and professional units via their representatives.

The Director of IT Services and Secretary to the College
The Director of IT Services and Secretary to the College are responsible for ensuring that cloud computing policy undergoes regular review to ensure alignment with evolving technical, security and compliance standards.

The Director of IT Services and Secretary to the College are responsible for promoting awareness of the policy among the University community.

Financial Services Department (FSD), IT Services & The Secretary's Office
The Financial Services department (FSD), IT Services & The Secretary's Office are responsible for providing professional services in the areas of procurement, legal compliance, data protection and cyber security to University personnel seeking to procure, implement or use cloud computing systems.

Cloud Computing Users

Cloud Computing Users are responsible for adhering to all cloud security guidelines and approved usage policies.

Cloud computing users must avail of any training provided for the cloud computing systems which they regularly use.

Cloud computing users must ensure that they are using only approved and vetted cloud systems for the processing and storage of University data. The use of personal cloud accounts for the storage and processing of University data is prohibited.

9. Related Documents

University Policies

The following University Policies may provide related information and guidance:

- Accessible Information Policy and Guidelines
- Business Continuity Management Policy
- Cookie Policy
- Data Protection Policy
- Ethics Policy
- Intellectual Property Policy
- IT and Cyber Security Policy
- Records Management Policy
- Trinity Policy on Good Research Practice
- Trinity Procurement Policy & Procedures
- Web Policy

Governmental Guidance Documents

The following guidance material released by the Irish Government may provide additional information.

- **Cloud Computing Advice Note 2025 -** *Department of Public Expenditure, NDP Delivery and Reform*
- **Cloud Services Procurement Guidance Note 2025 Update** - *Department of Public Expenditure, NDP Delivery and Reform*
- **Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies) in June 202315. -** *Department of the Environment Climate and Communications*

10. Document/version Control for New Policies

Approved by: Board
Date policy approved: 28 January 2015
Date of next review: 2030/31
Officer responsible for review: Director of IT Services

Document Control for Revised Policies

11.1 Date of initial approval: 28 January 2015
11.2 Date revised policy approved: 17 June 2026
11.3 Date policy effective from: 17 June 2026
11.4 Date of next review: Academic Year 2030/31