Policy Title:	MIE Policy on Cloud Computing Services
Description:	Policy stating MIE's commitment to ensuring that all its legal, ethical and policy compliance requirements are met in the procurement, evaluation and use of cloud services.
Author (Position):	Director of IT & e-Learning
Version:	1
Approved By:	MIE Governing Body
Policy Approval Date:	January 2019
Date of Next Policy Review:	April 2023 (or as necessary)

MIE Policy on Cloud Computing Services

1. Context

This document sets out the Marino Institute of Education's (MIE) policy for the use of cloud computing services, also known as cloud computing, cloud services or cloud.

1.1. Cloud Computing

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:

i. Infrastructure as a Service (IaaS);
ii. Software as a Service (SaaS);
iii. Platform as a Service (PaaS);
iv. Network as a Service (NaaS).

1.2. Cloud services are provided via four deployment models:

i. Private cloud – where services are provided by an internal provider i.e. IS Services;
ii. Public cloud – where services are provided by third parties i.e. external companies or entities, over the public Internet;
iii. Community cloud – where services are provided by external company(s) or entity(s) for a specific community of users with common interests;
iv. 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.
v. 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.

1.3. New challenges with Cloud Computing

i. 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 MIE, its staff, students and its agents are adequately protected at all times. The service must be selected to ensure that the data and information are secure and that an adequate backup and recovery plan are 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.

ii. 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 MIE, may inadvertently, and against MIE policy, purchase contracts with a cumulative value that exceeds procurement thresholds, breaching legislation.

iii. Historically, the steps involved in procuring and evaluating ICT services have rested with a multifunctional team of trained professionals in MIE's IT Team. 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 MIE staff or agents will bypass these professionals and the appropriate control procedures and put themselves and MIE at risk by procuring and/or using inappropriate cloud services.

2. Purpose

This policy is a statement of MIE'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. To whom does this policy apply?

This policy applies to all staff and students and to all agents or organisations acting for, or on behalf of, MIE in the evaluation, procurement or use of cloud services.

2.2. To what data and information does this policy apply?

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:

2.3. '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;

i. 'Sensitive personal data' 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;

ii. 'Confidential business data and information' is data and information which concern or relate 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 MIE, or other organisation, or other information of commercial value, the disclosure of which is likely to have the effect of either impairing MIE's ability to obtain such information as is necessary to perform its statutory functions, or causing substantial harm to the competitive position of MIE, or other organisation 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.

2.4. Data and Information classification

Personal data, sensitive personal data, and MIE's confidential business data and information are classified as shown below:

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 MIE website.	Term dates, dates of MIE closures, Staff names and contact details.	Access to this data is not usually restricted i.e. a username and password are not required to access this data.
	Institute Internal	Such data is generally available to all staff and students in MIE.	General meeting minutes, day to day activities and communications.	Access is usually restricted to members of MIE staff.
Confidential	Restricted	Such data is 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, and confidential information related to research or funding.	Access to this data is restricted to the people who 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 below.
	Critical	Such data is 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 MIE.	Information relating to the mental and physical health of individuals, data subject to a confidentiality clause, financial data such as bank account numbers and 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

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

i. Copyright and Related Rights Acts 2000, 2004 and 2007;

ii. Data Protection Acts 1988, 2003 and 2018;

iii. General Data Protection Regulation (GDPR);

iv. Freedom of Information Act 1997, 2003 and 2014;

v. Contract Law;

vi. EU Public Procurement Directives;

vii. The Child Trafficking and Pornography Acts 1998 and 2004;

viii. Defamation Act 2009;

ix. Prohibition of Incitement to Hatred Act 1989.

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

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

i. Data Protection & GDPR: Guidelines for External Examiners on European General Data Protection Regulation, 2018;

ii. Freedom of Information;

iii. Procurement; Purchasing of Goods and Procurement of Services

iv. Intellectual Property;

v. Ethics;

   a. Application for Ethical Approval of Research Proposals

   a. Ethics in Research Policy

   b. Procedure for Ethical Approval of Research Proposals

vi. Good Research Practice Policy;

vii. Accessible Information Policy;

viii. Use of MIE's trademarks;

ix. MIE Staff & Students Code of Conduct for Use of IT Systems;

x. MIE Website;

a. Marino Institute of Education Website(s) Terms of Use

b. MIE Policy on Management of MIE Website

c. MIE Website Cookies Policy

xi. Dignity and Respect Policy;

xii. MIE Policy on Social Media and Social Networking;

xiii. MIE Policy "Bring Your Own Device".

3.4. Criteria for all cloud services

All Cloud Services must:

i. Be fit for the purpose they are designed to support;

ii. Comply with all relevant Irish and European Legislation;

iii. Comply with all existing MIE Policies;

iv. Comply with Irish and European data protection legislation;

v. Respect the intellectual property rights of others and not breach copyright when using cloud services;

vi. Meet MIE Accessibility Requirements.

vii. Comply with the relevant professional ethics and with MIE's ethical principles. Where ethical issues arise in the use of cloud services, the guidance of the Institute's relevant committee must be sought in advance of the use of the service;

viii. Comply with the MIE's Good Research Practice Policy. Where necessary and appropriate, the guidance of the MIE's Ethics and Research Committee (MERC) must be sought before using a cloud service for research purposes.

ix. Comply with MIE Procurement procedures, evaluate and use of cloud service.

3.5. MIE 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 in relation to the cloud service under consideration.

MIE's IT Team must be contacted at evaluation stage for advice where data from a cloud service is required to integrate with an internal MIE system. Where integration is required, all MIE policies, procedures and project prioritisation must be adhered to;

3.6. Backup/Retention/Business Continuity/Disaster Recovery

i. The service must be selected to ensure that the data and information are 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 needs.

ii. For more critical systems, the service must be built with high availability, with a business continuity and disaster recovery plan that fits business needs. The IT Team must be contacted for advice and sign off in advance where a cloud services is being considered to provide a business critical IT system;

3.7. An appropriate formal contract must be put in place with the cloud service provider. It is generally not appropriate to simply accept the third party's generic terms and conditions.

MIE Procurement procedures must be consulted and provide written sign off in advance to ensure that appropriate contract law, procurement legislation and MIE policies are adhered to.

3.8. For a New Cloud Service:

i. The individual or agent must ensure that all criteria for cloud services have been met and submit their checklist to the President of MIE and the Director of IT & e-Learning so the service can be evaluated;

ii. Approval must be obtained from the President of MIE and the Director of IT & e-Learning or their appointed nominees before a new service can be purchased or used for the first time;

iii. Approval must be obtained from the President of MIE and the Director of IT & e-Learning or their appointed nominees before using an approved MIE cloud service if the service has not been approved for the classification of data and information under consideration;

iv. If the service is a new cloud service, and passes all the above steps, then the President of MIE and the Director of IT & e-Learning will designate the service a MIE approved cloud service, for the given classification of data and information.

4. Policy Compliance and Handling of Policy Breaches

4.1. The President of MIE and the Director of IT & e-Learning, or their appointed nominees, reserve the right to refuse MIE 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;

4.2. The President of MIE and the Director of IT & e-Learning must be notified in writing of all cloud services procured and in use by staff, students or agents of MIE that hold MIE data and information or that have been procured on behalf of MIE;

4.3. In exceptional circumstance, having due regard for the appropriate legislation and policies, the President of MIE and the Director of IT & e-Learning may authorise derogations from this policy;

4.4. Where it is alleged that a breach of policy has occurred the matter should be reported by the complainant to the President of MIE and the Director of IT & e-Learning. Thereafter, in consultation with President of MIE, the Director of IT & e-Learning, and Human Resources, 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 disciplinary procedure.

5. Responsibility

Director of IT & e-Learning, and other members of the IT Team in MIE have responsibility for this document and its implementation, as appropriate.

6. Related Documents

6.1 Purchasing of Goods and Procurement of Services

6.2 Disciplinary Policy

6.3 Marino Institute of Education Privacy Statement

6.4 Guidelines for External Examiners on European General Data Protection Regulation, 2018

6.6 Application for Ethical Approval of Research Proposals

6.7 Ethics in Research Policy

6.8 Procedure for Ethical Approval of Research Proposals

6.9 Good Research Practice Policy

6.10 Accessible Information Policy

6.11 MIE Staff & Students Code of Conduct for Use of IT Systems;

6.12 Marino Institute of Education Website(s) Terms of Use

6.13 MIE Policy on Management of MIE Website

6.14 MIE Website Cookies Policy

6.15 Dignity and Respect Policy

6.16 MIE Policy on Social Media and Social Networking

6.17 MIE Policy “Bring Your Own Device"