TITLE: ***IT POLICY***

Effective Date	16 January 2019	**Version**	02
Approved By	Management Board	**Date Approved**	16 January 2019
		Review Date	16 January 2022 *or as required*
Superseded or Obsolete Policy / Procedure(s)		**Owner:**	
01 – *IT Policy* (2011)		IT Services	

1. Purpose of Policy

Carlow College, St. Patrick's (hereafter Carlow College) is committed to providing an Information Technology (IT) computing resource for learners and staff to support the normal activities of the College for educational, research and administrative purposes.

The requirement and necessity for an IT policy has been identified through Quality Assurance standards and risk management to safeguard essential computing resources / services, protect the privacy of its learners and staff and comply with contractual requirements and legislation. The purpose of this high-level *IT Policy* and referenced policies, covering specific computing areas, is to provide direction, coordination, management and protection of all IT computing resources and services within Carlow College. This is achieved through maintaining the highest standards in implementing appropriate computing resources and providing procedures and guidelines thereafter for their successful operation. It is the responsibility of all learners and staff to be aware of and adhere to this Policy and other subsequent policies and procedures.

The *IT Policy* allows for progression, growth and investment in the IT infrastructure within the College. The *IT Policy* takes into consideration guidelines for risk management and control frameworks such as Data Governance DAMA DMBOK Framework and Information Security with consideration also given to ISO 27000 series standards and guidelines, General Data Protection Regulations (GDPR) and Payment Credit Card Industry (PCI) compliance. The IT Office is dedicated to implementing all advances in IT in line with the business requirements teaching and learning objectives of Carlow College.

2. Definitions

DAMA – Data governance practices of data management through research, education, publications, promotion of standards.

ISO 27000 series – recommended industry standards and guidelines for information security.

PCI Compliance – Payment Card industry data security for card/electronic payments.

DAMA DMBOK – collection of processes and knowledge areas that are generally accepted as best practices within the Data Management discipline.

3. Scope of Policy

The *IT Policy* incorporates the acceptable usage of all IT infrastructure, critical assets, and network resources by relevant stakeholders which include staff, learners and any authorised third parties on Carlow College Campus. This will include network facilities, data systems such as the Student Records Management System (SRMS) and Virtual Learning Environment (VLE), Wi-Fi use, all electronic computing devices and printing facilities. The policy is applicable to any and every member of Carlow College community including, but not limited to, faculty, learners, administrative officials, staff and independent contractors. The scope of this policy will also set expectation guidelines for stakeholders to carry out IT activities responsibly to ensure the security and protection of critical data/information of Carlow College.

4. Policy Statement

Carlow College recognises their responsibility and the underlying principles to ensure best practice for protection, management and security of data, core assets and functions of the College through IT. The objective of the *IT Policy* is to support all associated IT procedures, guidelines and security strategies in line with the overall mission of the College.

The following general principles must be applied in all IT related projects and operations:

- Carlow College is committed to meeting the technological and digital needs of the organisation to carry out daily operational functions through technology infrastructure including networks, hardware, software and storage for processing of critical data.
- Carlow College recognises their responsibility to protect the confidentiality, integrity and availability of organisational data through mitigation of security vulnerabilities.
- Measures are taken by all **staff** and **learners** to ensure that the IT systems are being used in a professional and ethical manner to maintain high standards within the College. Failure to do so could potentially lead to any of the following:
    - Financial Loss
    - Loss of Critical College Data
    - Damage to the Reputation of the College
    - Legal Consequences
    - Security requirements are mandatory wherever they are applicable and

The *IT Policy* and supporting policies relate to use of:

a. All College networks connected to the Server;

b. All College-owned/leased/rented and on-loan facilities;

c. To all private systems, owned/leased/rented/on-loan, when connected to the College network directly, or indirectly;

d. To all College-owned/licensed data/programs, on College and on private systems;

e. To all data/programs provided to the College by sponsors or external agencies.

Employees found to be abusing this policy and its subsequent and related practices and procedures will be subject to the organisations disciplinary action up to and including dismissal.

5. Roles and Responsibilities

5.1 IT Officer Responsibilities

The IT Officer is the owner of this policy and is responsible for applying all associated policies and guidelines to include:

- Provide training resources and awareness facilitation.
- To contribute to the development of policies which support the IT infrastructure.
- To define and implement standards and procedures which enforce agreed policies.
- To initiate regular reviews and ensure documentation is updated as appropriate.
- To provide secure mechanisms for central storage of all Documentation.
- To regularly audit and review the technological requirements of the organisation to continue to efficiently support the daily technological operations needs of the college.
- To liaise with the Director of Operations and through him, with the board of management on all matters relating to operational development and expansion of IT infrastructure.

5.2 Management Responsibilities

- Ensuring the *IT Policy* and all related policies are implemented and adhered to in their area.
- Reporting any breach of the *IT Policy* to IT Services.
- Report any changes within their area which may impact the *IT Policy*, such as change in process or operational procedures relating to use of network infrastructure.

5.3 Staff Responsibilities

All staff and external parties using IT resources within Carlow College are expected to adhere to all IT policies and related documents at all times.

6. Referenced Policies

In support of the high-level *IT Policy*, the following documents are currently under review:

- *Access Management Policy*
- *Data Protection Policy*

- *Disciplinary Policy (Staff)*
- *Information Security Policy*
- *Learner Code of Conduct and Disciplinary Policy*
- *Records Management Policy*
- *Remote Working Policy*
- *Social Networking and Social Media Policy*
- *Social Networking and Social Media Policy for Learners*

7. Monitoring and Review

This policy will be reviewed annually to ensure due care and due diligence under IT regulation and security requirements. Due to the increasing evolution of technology, there will be ongoing auditing of the technological platform to ensure college systems and fit for purpose.