COLÁISTE CHEATHARLACH
NAOMH PÁDRAIG
CARLOW COLLEGE
ST. PATRICK'S

**TITLE:** ***INFORMATION SECURITY POLICY***

| | | | |
|---|---|---|---|
| **Version** | 2 | **Date Approved** | 15 May 2024 |
| | Policy revised as part of the introduction of a comprehensive Information Security Management System at Carlow College, St. Patrick's; a system that aligns to ISO27001. This policy also replaces the *IT Policy*, which was originally approved in 2011. | **Review Date** | 15 May 2027 *or as required* |
| **Approved By** | Management Board | | |
| **Owner** | Information Security Management Review Team | | |

| **Version Control** | | |
|---|---|---|
| **Version No.** | **Date Approved** | **Documented Changes** |
| 1 | 6 February 2019 | Initial Issue |

## 1. Purpose of Policy

The purpose of the *Information Security Policy* is to set out the information security policies that apply to Carlow College, St. Patrick's (hereafter Carlow College), to protect the confidentiality, integrity, and availability of data. This policy is part of the Carlow College Information Security Management System (ISMS), which is aligned to ISO 27001. A key objective of this policy is to define security controls necessary to safeguard Carlow College information systems and physical environments and ensure that information held therein is held securely and uncompromised.

Although not an exhaustive list of legislation, this policy has several statutory obligations: *Data Protection Act 2018*, General Data Protection Regulation (GDPR), *Qualifications and Quality Assurance (Education and Training (Amendment) Act 2019*, *Freedom of Information Act 2014*, *Criminal Damages Act 1997*, *Child Trafficking and Pornography Act 1998*, *Intellectual Property Miscellaneous Act 1998*, *Copyright and Related Rights Act 2000 (as amended)* and *Electronic Commerce Act 2000*.

## 2. Definitions

*Contractor* – an individual or business that is hired to do a specific job or task for Carlow College. Contractors are not employees, but are instead hired through a contractual agreement to complete a specific task or project. Contractors may be hired to do short-term or long-term work, and may be hired for a specific skill or expertise that is needed for a project. Contractors are paid on a per-project basis, and are not entitled to benefits or other employment-related perks that employees typically receive.

*Employee* – a worker that performs specific tasks for Carlow College in exchange for regular pay. Employees negotiate a salary with their employer and typically receive benefits, including overtime and holiday pay. An employee is engaged by Carlow College to perform services under the guidance and supervision of the employer. These tasks are generally part of the core operations of the business. The employer will control the place, hours, and method of work.

*Information* – any data or knowledge that is created, received, stored, transmitted, disposed of or otherwise used or processed within an organisation, and constitutes evidence of the organisation's functions and activities. Organisations process information in many forms, including electronic, physical and verbal (e.g. conversations and presentations). The terms 'information' and 'data' are often used interchangeably in common usage.

*Information Security* – defined as preserving:

| | |
|---|---|
| **Confidentiality** | Access to information is to those with appropriate authority<br>***The right people with the right access*** |
| **Integrity** | Information is complete and accurate |

| | |
|---|---|
| **Availability** | ***to the right data*** |
| | Information is available when it is needed ***at the right time*** |

*Information Security Management* Review *Team* is appointed by the Management Board and is responsible for ensuring the effective delivery of the ISMS and its continual improvement. This Team includes representatives from the following areas: Senior Management, IT & Student Systems, Data Protection, Human Resources, Facilities and Academic Affairs (see Appendix 2 for terms of reference).

*Third-Party Users* – are people or organisations needing access to Carlow College's site without the requirement to be a permanent user of the user base. A third-party user can also be a company or individual outside Carlow College that performs activities for the College; this can include voluntary workers and non-Carlow College work placement learners.

## 3. Scope of Policy

This policy applies to: all employees and learners of Carlow College, third-party users or contractors.

## 4. Policy Statement

Information security is managed based on assessment of risk, legal and regulatory requirements, and business need.

### *4.1 President's Statement of Commitment*

As a College, information processing is fundamental to our success and the protection and security of that information is a priority of the Management Board. Carlow College takes its obligations under legislation seriously. *Carlow College* has provided the resources to develop, implement and continually improve the ISMS appropriate to our business. **Fr Conn Ó Maoldhomhnaigh, President, Carlow College St, Patrick's, 15 May 2024.**

### *4.2 Introduction*

Information security protects the information that is entrusted to Carlow College. Getting information security wrong can have significant adverse impacts on our employees, our learners, our reputation, and our finances. By having an effective ISMS, we can:

- provide assurances for our legal, regulatory, and contractual obligations;
- ensure the right people, have the right access to the right data at the right time;
- assist with the protection of personal data as defined by the GDPR; and
- be good data citizens and custodians.

### *4.3 Information Security Objectives*

The following are the Information Security Objectives for the College:

- to ensure the confidentiality, integrity and availability of College information including, but not limited to, personal data as defined by the GDPR based on good risk management, legal regulatory and contractual obligations, and business need;
- to provide the resources required to develop, implement, and continually improve the ISMS;
- to effectively manage third party suppliers who process, store, or transmit information to reduce and manage information security risks; and
- to implement a culture of information security through effective training and awareness.

### *4.4 Information Security Policy Framework*

The ISMS is built upon an information security policy framework. For a complete list of policies related to the Information Security Management Framework at Carlow College, visit: www.carlowcollege.ie/information-security.

The following policies are associated with the ISMS, but they are not managed by the Information Security Management Review Team:

- *Assessment of Learners Policy*
- *Critical Incident Policy*
- *Freedom of Information Policy*
- *Health and Safety Policy*
- *Quality Assurance Policy*
- *Social Networking and Social Media Policy for Staff*
- *Social Networking and Social Media Policy for Learners*

- *Teaching and Learning Policy*

### *4.5 Information Security Roles and Responsibilities*

Information security is the responsibility of everyone to understand and adhere to the policies, follow process and report suspected or actual breaches. Specific roles and responsibilities for the running of the ISMS are defined and recorded in the document *Information Security Roles Assigned and Responsibilities* (this document is kept and monitored by the Information Security Management Review Team). All training related to the ISMS is governed by the *Information Security Awareness and Training Policy*.

### *4.6 Monitoring*

Compliance with the policies and procedures of the ISMS is monitored via the Information Security Management Review Team, together with independent reviews by both Internal and External Audit on a periodic basis.

### *4.7 Legal and Regulatory Obligations*

The organisation takes its legal and regulatory obligations seriously and these requirements are recorded in the document *Legal and Contractual Requirements Register* (this document is kept and monitored by the Information Security Management Review Team).

### *4.8 Training and Awareness*

Policies are made readily and easily available to all employees, learners and third-party users and are integrated with the College's Quality Assurance Framework. All training related to the ISMS is governed by the *Information Security Awareness and Training Policy*. The central objective of this training is to communicate the policies, processes and concepts of information security.

### *4.9 Continual Improvement of the Management System*

The ISMS is continually improved. The *Continual Improvement Policy* sets out the College approach to continual improvement and there is continual improvement process in place.

### *4.10 Protection of Personal Data*

Carlow College processes personal data about employees, learners, and other data subjects for various purposes, including academic, administrative and commercial purposes. When handling such information, the College, and all staff or others who process or use any personal data, must comply with the data protection principles, which are set out in Data Protection law. This includes, but is not limited to, the GDPR. Responsibilities under Data Protection law are set out in the *Data Protection Policy*.

## 5. Responsibilities

It is the responsibility of all employees, contractors, third-party users and learners to report suspected breaches of this policy without delay to:

- During Normal Business Hours: Relevant Key Personnel OR Dial the Incident Number at Carlow College +353 86 2018268.
- Outside Normal Business Hours: Dial the Incident Number at Carlow College +353 86 2018268.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with College disciplinary procedures.

### *5.1 Employees*

It is the responsibility of College employees to safeguard Carlow College information systems and physical environments and ensure that information held therein is held securely and uncompromised.

### *5.2 Learners*

It is the responsibility of College learners to safeguard Carlow College information systems and physical environments and ensure that information held therein is held securely and uncompromised.

### *5.3 Third-Party Users and Contractors*

It is the responsibility of third-party users and contractors to safeguard Carlow College information systems and physical environments and ensure that information held therein is held securely and uncompromised.

### *5.4 Management Board*

The Management Board is responsible for approving all policies related to the ISMS, as outlined in the College's *Policy on Policies*. Moreover, the Management Board is responsible for ensuring that the Information Security Management Review Team complies with its terms of reference and ensures that all areas of the College are compliant with the ISMS.

### *5.5 Information Security Management Review Team*

The Information Security Management Review Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved and recorded by the Information Security Management Review Team and reported to the Management Board. For more on the Information Security Management Review Team, see Appendix 2: *Terms of Reference*.

## 6. Referenced Policies

See Section 4.4 above.

## 7. Associated Documents

- Appendix 1: Areas of the IS27001 Standard Addressed
- Appendix 2: Information Security Management Review Team Terms of Reference

For a complete list of policies related to the Information Security Management Framework at Carlow College, visit: www.carlowcollege.ie/information-security.

## 8. Monitoring and Review

This Policy will be reviewed annually and regularly updated as necessary if and when organisational structure or business practices and processes change. As part of our internal Quality Assurance Framework, this policy will be formally reviewed every three years (upon first approval) and every five years thereafter.

## Appendix 1: Areas of the IS27001 Standard Addressed

# Areas of the IS27001 Standard Addressed

| ISO27001:2022 | ISO27002:2022 | ISO27001:2013/2017 | ISO27002:2013/2017 |
|---|---|---|---|
| ISO27001:2022 Clause 5 Leadership<br><br>ISO27001:2022 Clause 5.1 Leadership and commitment<br><br>ISO27001:2022 Clause 5.2 Policy<br><br>ISO27001:2022 Clause 6.2 Information security objectives and planning to achieve them<br><br>ISO27001:2022 Clause 7.3 Awareness | ISO27002:2022 Clause 5 Organisational Controls<br><br>ISO27002:2022 Clause 5.1 Policies for information security<br><br>ISO27002:2022 Clause 5.36 Compliance with policies, rules, and standards for information security<br><br>ISO27002:2022 Clause 5.4 Management Responsibilities<br><br>ISO27002:2022 Clause 6 People Controls<br><br>ISO27002:2022 Clause 6.3 Information security awareness, education, and training<br><br>ISO27002:2022 Clause 6.4 Disciplinary process | ISO27001:2013/2017 Clause 5 Leadership<br><br>ISO27001:2013/2017 Clause 5.1 Leadership and commitment<br><br>ISO27001:2013/2017 Clause 5.2 Policy<br><br>ISO27001:2013/2017 Clause 6.2 Information security objectives and planning to achieve them<br><br>ISO27001:2013/2017 Clause 7.3 Awareness | ISO27002:2013/2017 Clause 5 Information security policies<br><br>ISO27002:2013/2017 Clause 5.1 Management direction for information security<br><br>ISO27002:2013/2017 Clause 5.1.1 Policies for information security<br><br>ISO27002:2013/2017 Clause 5.1.2 Review of the policies for information security<br><br>ISO27002:2013/2017 Clause 7 Human resource security<br><br>ISO27002:2013/2017 Clause 7.2.1 Management Responsibilities<br><br>ISO27002:2013/2017 Clause 7.2.2 Information security awareness, education, and training<br><br>ISO27002:2013/2017 Clause 7.2.3 Disciplinary process |

**Appendix 2: Information Security Management Review Team Terms of Reference**

COLÁISTE CHEATHARLACH
NAOMH PÁDRAIG
CARLOW COLLEGE
ST. PATRICK'S

# Terms of Reference
## *Information Security Management Review Team*

### Section 1: Remit

The Information Security Management Review Team is responsible for ensuring the effective delivery of the Information Security Management System (ISMS) and its continual improvement. The ISMS at Carlow College, St. Patrick's (hereafter Carlow College) has been established to align with ISO 27001. To meet this standard, the policies that form part of this framework require that the Information Security Management Review Team to:

- systematically examine the College's information security risks, taking account of the threats, vulnerabilities, and impacts;
- design and implement a coherent and comprehensive suite of information security controls and / or other forms of risk treatment (such as risk mitigation, avoidance or transfer) to address those risks that are deemed unacceptable; and
- adopt an overarching management process to ensure that the information security controls continue to meet the College's information security needs on an ongoing basis.

All policies and procedures that form part of the ISMS must comply with international and national best practice and relevant legislation.

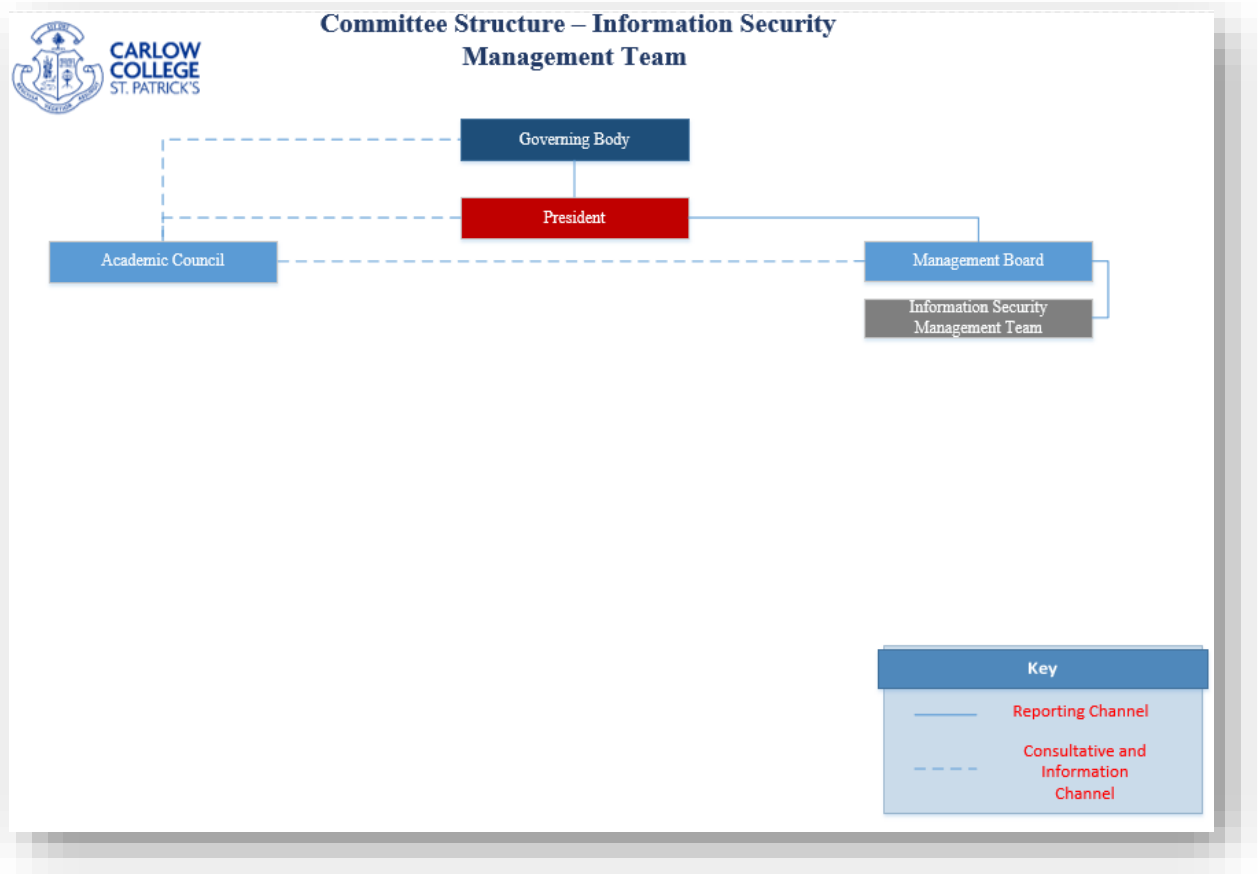
### Section 2: Membership

The members of the Information Security Management Review Team are on the Team by virtue of their function within Carlow College. In general terms, they represent key operational areas within Carlow College.

| Function | Mode of Selection |
|---|---|
| Senior Management Review Team Representative, Chair | Appointed by the Management Board *(ex officio)* |

| | |
|---|---|
| Head of IT | *Ex officio* |
| Data Protection Officer | *Ex officio* |
| Head of Human Resources and EDI | *Ex officio* |
| Head of Facilities | *Ex officio* |
| Head of Academic Delivery and Programmes | *Ex officio* |

## Section 3: Reporting Structure




The Information Security Management Review Team reports directly to the Management Board. To comply with the Quality Assurance Framework at Carlow College, all policies managed by the Information Security Management Review Team are approved by the Management Board and updates regarding its activities are reported twice each semester.

## Section 4: Terms of Reference

The Information Security Management Review Team is tasked with:

- create and keep records of meetings adhering to the *Records Management Policy*;
- to develop the decision-making process within the Information Security Management Team;
- to ensure that all documents related to the management of the ISMS are reviewed quarterly, the documents include: Competency Matrix, Documented ISMS Scope Statement, Statement of Applicability, Communication Plan, ISMS Management Plan, ISMS Document Tracker, Information Security Roles Assigned and Responsibilities, Legal and Contractual Requirements Register, Training and Awareness Plan; Controls Accountability Matrix and Information Security Risk Register;
- to ensure that policies related to the ISMS are monitored and reviewed according to what is stated in the policy;
- to ensure that all standard operating procedures, at the departmental level, are developed, and maintained, in accordance with relevant policies;
- submit updates to the Management Board at least twice a semester; and
- to conduct frequent internal audits of the ISMS and engage with the appointed auditor of the College annually and respond to their recommendations.

**Section 6: Quorum**

The quorum for a meeting shall be fifty percent plus one of the current membership of the Information Security Management Team, one of whom shall be the Chair.

**Section 7: Voting at Meetings**

All decisions of the Information Security Management Team shall normally be carried by consensus. However, where this is not possible, a simple majority of votes shall decide, and in the case of equality of votes, the Chair shall have a second or casting vote.

**Section 8: Frequency of Meetings**

The Information Security Management Team shall meet annually in late August and at least twice each semester. As the ISMS is being developed, the frequency of meetings will be more frequent.