COLÁISTE CHEATHARLACH
NAOMH PÁDRAIG
CARLOW COLLEGE
ST. PATRICK'S

TITLE: *ACCEPTABLE USE POLICY*

<table>
<tr><td rowspan="2"><b>Version</b></td><td colspan="2">2</td><td colspan="2"><b>Date Approved</b></td><td>15 May 2024</td></tr>
<tr><td colspan="2">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 further replaces the <i>Internet and Email Usage Policy</i>, which was initially approved on 20 March 2019.</td><td colspan="2"><b>Review Date</b></td><td>15 May 2027 <i>or as required</i></td></tr>
<tr><td><b>Approved By</b></td><td colspan="5">Management Board</td></tr>
<tr><td><b>Owner</b></td><td colspan="5">Information Security Management Review Team</td></tr>
<tr><th colspan="6">Version Control</th></tr>
<tr><td><b>Version No.</b></td><td><b>Date Approved</b></td><td colspan="4"><b>Documented Changes</b></td></tr>
<tr><td>1</td><td>20 March 2019</td><td colspan="4">Initial Issue (original title was <i>Internet and Email Usage Policy</i>)</td></tr>
<tr><td>1.1</td><td>11 May 2022</td><td colspan="4">Policy re-approved for six months and will be reviewed as part of ISO standards.</td></tr>
<tr><td>1.2</td><td>3 May 2023</td><td colspan="4">Policy re-approved until 30 September 2023 and will be reviewed as part of ISO standards.</td></tr>
</table>

1. Purpose of Policy

The purpose of the *Acceptable Use Policy* is to make employees, learners, third-party users and contractors aware of the rules for the acceptable use of assets associated with information and information processing. This policy is part of the Carlow College, St. Patrick's (hereafter Carlow College) Information Security Management System, which is aligned to ISO27001.

2. Definitions

Contractor – is 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.

Data Owner – the person accountable for data assets in their area and authorises use of that data.

Devices – include, but are not limited to laptop computers, desktop computers, registered servers, tablet devices, smartphones, internet connected devices that are commonly referred to as "IOT" or "Internet of Things" and external storage devices regardless of whether the device was purchased by the College or is personally owned.

Email System – the technology system used for transmission of electronic messages over a communications network.

Employee – is 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.

Intellectual Property – creations of the mind, such as inventions; literary and artistic works, designs; and symbols, names and images used in commerce. Intellectual Property is protected in law by, for example, patents, copyright and trademarks.

Internet System – the worldwide network of computers and networks accessible from a single PC or device.

Third-Party Users – are people or organisations needing access to Carlow College 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 of Carlow College, learners of Carlow College, third-party users and contractors.

4. Policy Statement

The fundamental principle that the *Acceptable Use Policy* uses is that the use of assets is in line with applicable legislation, College policies and is in place to safeguard the College data, employees and learners. Each user is to be responsible for their own actions and act responsibly and professionally. Please note that College email, accounts and devices are for College use only.

4.1 Individual Responsibility

Access to the IT systems is controlled using User IDs, passwords and / or tokens. All User IDs and passwords are to be uniquely assigned to named individuals, and consequently, individuals are accountable for all actions on the College IT systems.

Individuals must not:

- allow anyone else to use their user ID / token and password on any College IT system;
- leave their user accounts logged in at an unattended and unlocked computer;
- use someone else’s user ID and password to access College IT systems;
- leave their password unprotected (for example, by writing it down);
- perform any unauthorised changes to College IT systems or information;
- attempt to access data that they are not authorised to use or access;
- exceed the limits of their authorisation or specific business need to interrogate the system or data;
- connect any personal device that has not been authorised to connect to the Carlow College network or IT systems;
- store College data locally on devices; instead, College data should be stored on the relevant system provided by the College like the Cloud; and
- give or transfer College data or software to any person or organisation outside the College without the authorisation of the College.

All users must ensure that individuals are given clear direction on the extent and limits of their authority about IT systems and data.

4.2 Internet and Email Usage

Use of the College internet and email is intended for business use by employees and relevant third parties, and by learners in connection with their programme of study. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the College in any way, not in breach of any term and condition of employment or College policies, terms of conditions of registration and does not place the individual or the College in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must **not**:

- send or store Carlow College payment card information such as:
  - payment card number (Primary Account Number or PAN);
  - security code (CVV2 etc.); and / or
  - start and expiry dates.
- use the internet or email for the purposes of harassment or abuse;
- use profanity, obscenities, or derogatory remarks in communications;
- access, download, send or receive any data (including images), which the College considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material;
- use the internet or email to make personal gains or conduct a personal business;
- use the internet or email to gamble;
- use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam;
- send unprotected sensitive, internal, or confidential information both internally and / or externally;
- send / forward the College mail or College-owned data / information to personal (non-College) email accounts (for example a personal cloud or owned domain account);
- make official commitments through the internet or email on behalf of the College unless authorised to do so;
- download any copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval;
- in any way infringe any copyright, database rights, trademarks, or other intellectual property;

- download or install or distribute any software from the internet without prior approval of the IT Department; and / or

- connect the College devices to the internet using non-standard connections.

4.3 Working Off Site

It is accepted that College mobile devices and information may be taken off-site (see the *Information Classification and Handling Policy* for further guidance). The following controls must be applied:

- working away from the office must be in line with the College's *Hybrid Working Policy*;

- laptop and mobile device encryption must be used;

- laptop and mobile devices must also be protected at least by a password or a PIN;

- equipment and media taken off-site must not be left unattended in public places including on public transport and not left in sight in a car;

- laptops and mobile devices must be carried as hand luggage when travelling; and

- information should be protected against loss or compromise when working remotely (for example at home or in public places).

4.4 Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives are not to be used unless authorised and where strictly necessary. Storage of information within systems and electronic transfer are the preferred practices. Only College owned, managed, and authorised mobile storage devices with encryption enabled must be used, when transferring internal or confidential data. Please see the *Information Classification and Handling Policy* for more information on the classification and handling of information and data.

4.5 Monitoring and Filtering

All data that is created and stored on College computers is the property of the College, however, wherever possible, the College will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The College has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, and any other applicable legislation (see Appendix 2: Guidelines for Monitoring the IT Environment).

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

All employees have a responsibility to use assets is in line with applicable legislation, College policies and is in place to safeguard the College data. As such, each employee is to be responsible for their own actions and act responsibly and professionally.

5.2 Learners

All learners have a responsibility to use assets is in line with applicable legislation, College policies and is in place to safeguard the College data. As such, each learner is to be responsible for their own actions and act responsibly and professionally.

5.3 Third-Party Users and Contractors

All third-party users and contractors have a responsibility to use assets is in line with applicable legislation, College policies and is in place to safeguard the College data. As such, each third-party user and contractor is to be responsible for their own actions and act responsibly and professionally.

5.4 IT

It is the responsibility of IT to monitor the IT Environment according to the guidelines outlined in this policy (see Appendix 2).

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.

6. Referenced Policies

- *Access Control Policy*
- *CCTV Policy*
- *Child Protection Policy*
- *Clear Desk and Clear Screen Policy*
- *Data Protection Policy*
- *Disciplinary Policy* (Staff)
- *Equality Policy*
- *Freedom of Information Policy*
- *Hybrid Working Policy*
- *Information Classification and Handling Policy*
- *Information Security Policy*
- *Learner Code of Conduct and Disciplinary Policy*
- *Library Admission and User Services Policy*
- *Physical and Environmental Security Policy*
- *Social Media and Networking Policy (Staff)*
- *Social Networking and Social Media Policy for Learners*
- *Staff Code of Conduct Policy*

7. Associated Documents

- Appendix 1: Acceptable Use Policy: Relevant ISO27001 Controls Mapping

- Appendix 2: Guidelines for Monitoring the IT Environment

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: Acceptable Use Policy: Relevant ISO27001 Controls Mapping

Acceptable Use Policy Relevant ISO27001 Controls Mapping

ISO27001:2022	ISO27002:2022	ISO27001:2013/2017	ISO27002:2013/2017
ISO27001:2022 Clause 5 Leadership ISO27001:2022 Clause 5.1 Leadership and commitment ISO27001:2022 Clause 5.2 Policy ISO27001:2022 Clause 6.2 Information security objectives and planning to achieve them ISO27001:2022 Clause 7.3 Awareness	ISO27002:2022 Clause 5 Organisational Controls ISO27002:2022 Clause 5.1 Policies for information security ISO27002:2022 Clause 5.36 Compliance with policies, rules, and standards for information security ISO27002:2022 Clause 5.3 Segregation of Duties ISO27002:2022 Clause 5.4 Management Responsibilities ISO27002:2022 Clause 5.9 Inventory of information and other associated assets ISO27002:2022 Clause 5.10 Acceptable use of information and other associated assets ISO27002:2022 Clause 5.11 Return of Assets ISO27002:2022 Clause 5.15 Access Control ISO27002:2022 Clause 5.18 Access Rights ISO27002:2022 Clause 5.32 Intellectual Property ISO27002:2022 Clause 5.33 Protection of Records ISO27002:2022 Clause 5.34 Privacy and protection of PII ISO27002:2022 Clause 6 People Controls ISO27002:2022 Clause 6.7 Remote Working ISO27002:2022 Clause 7 Physical Security	ISO27001:2013/2017 Clause 5 Leadership ISO27001:2013/2017 Clause 5.1 Leadership and commitment ISO27001:2013/2017 Clause 5.2 Policy ISO27001:2013/2017 Clause 6.2 Information security objectives and planning to achieve them ISO27001:2013/2017 Clause 7.3 Awareness	ISO27002:2013/2017 Clause 5 Information security policies ISO27002:2013/2017 Clause 5.1 Management direction for information security ISO27002:2013/2017 Clause 5.1.1 Policies for information security ISO27002:2013/2017 Clause 5.1.2 Review of the policies for information security ISO27002:2013/2017 Clause 6.1.2 Segregation of Duties ISO27001:2013/2017 Clause 8 Asset Management ISO27001:2013/2017 Clause 8.1 Responsibility for Assets ISO27001:2013/2017 Clause 8.1.1Inventory of Assets ISO27001:2013/2017 Clause 8.1.2 Ownership of Assets ISO27002:2013/2017 Clause 8.1.3 Acceptable Use of Assets ISO27002:2013/2017 Clause 8.1.4 Return of Assets ISO27002:2013/2017 Clause 8.2.3 Handling of Assets ISO27002:2013/2017 Clause 8.3.2 Disposal of Media ISO27002:2013/2017 Clause 9.2.5 Review of User Access Rights ISO27002:2013/2017 Clause 11 Physical and Environmental

	ISO27002:2022 Clause 7.1 Physical Security Perimeter ISO27002:2022 Clause 7.9 Security of assets off-premises ISO27002:2022 Clause 7.13 Equipment maintenance ISO27002:2022 Clause 7.14 Secure disposal or re-use of equipment ISO27002:2022 Clause 8 Technological Controls ISO27002:2022 Clause 8.1 User Endpoint Devices ISO27002:2022 Clause 8.3 Information access restriction ISO27002:2022 Clause 8.8 Management of technical vulnerabilities ISO27002:2022 Clause 8.10 Information Del		ISO27002:2013/2017 Clause 11.2 Equipment ISO27002:2013/2017 Clause 11.2.4 Equipment maintenance ISO27002:2013/2017 Clause 11.2.5 Removal of assets ISO27002:2013/2017 Clause 11.2.6 Security of equipment and assets off premises ISO27002:2013/2017 Clause 11.2.7 Secure disposal of equipment ISO27002:2013/2017 Clause 11.2.8 Unattended User equipment ISO27002:2013/2017 Clause 12 Operations Security ISO27002:2013/2017 Clause 12.6.1 Management of technical vulnerabilities ISO27002:2013/2017 Clause 12.6.2 Restrictions on software installation ISO27002:2013/2017 Clause 15 Supplier Relationships ISO27002:2013/2017 Clause 15.1 Information Security in Supplier Relationships ISO27002:2013/2017 Clause 18 Compliance ISO27002:2013/2017 Clause 18.1.2 Intellectual Property rights ISO27002:2013/2017 Clause 18.1.3 Protection of Records ISO27002:2013/2017 Clause 18.1.4 Privacy and protection of personally identifiable information

Appendix 2: Guidelines for Monitoring the IT Environment

COLÁISTE CHEATHARLACH
NAOMH PÁDRAIG
CARLOW COLLEGE
ST. PATRICK'S

Guidelines for Monitoring the IT Environment

A. Monitoring Principles

The following must be observed when monitoring the IT environment:

1. **Clear Objectives:** Defined purposes and goals of monitoring the IT environment including system availability, identifying performance bottlenecks, detecting security threats, and optimising resource utilisation.

2. **Key Metrics:** Determined critical parameters to monitor based on the College's priorities and IT infrastructure. This includes metrics related to network traffic, server performance, application response times, security events, and more.

3. **Monitoring Tools:** Strategic investments plus Standard monitoring tools that align with the identified metrics and objectives. In-built tools that provide real-time monitoring, historical data analysis, customizable alerts, and scalability to meet future needs.

4. **Monitoring Plans:** Detailed monitoring plans for each aspect of the IT environment, including servers, networks, applications, databases, and security systems.

5. **Configure Alerts and Notifications:** Set-up of alerts and notifications to promptly detect and respond to abnormal conditions or potential issues in the IT environment. Determined thresholds for each metric to trigger alerts and establish escalation procedures for critical incidents.

6. **Established Baselines:** Established baseline performance metrics to understand normal operating conditions and deviations from the norm. Baselines help in identifying anomalies and performance trends over time.

7. **Regular Review and Analysis:** Conduct regular reviews and analysis of monitoring data to identify patterns, trends, and potential areas for improvement. Use of historical data to forecast future needs and optimise resource allocation.

8. **Documentation and Reporting:** Maintain detailed documentation of monitoring configurations, alerts, incidents, and resolutions. Generate regular reports to communicate the status of the IT environment to stakeholders, management, and other relevant parties.

9. **Continuous Improvement:** Continuously evaluate and improve monitoring processes and tools to adapt to changing technology landscapes, business requirements, and security threats. Seek feedback from stakeholders and incorporate lessons learned from incidents.

10. **Compliance and Security:** Ensure that monitoring practices comply with relevant regulations and standards, particularly concerning data privacy and security. Implement measures to safeguard monitoring data and prevent unauthorised access.

B. Description of IT Environments

1. Network Infrastructure: Carlow College monitor network traffic, bandwidth utilisation, latency, and packet loss to ensure smooth communication between devices and detect potential issues affecting connectivity or performance.

2. Server Infrastructure: Carlow College monitoring includes server health, resource utilisation (CPU, memory, disk), uptime, and service availability. The College will proactively identify and address any issues that may impact the performance or availability of critical services.

3. Application Performance: Carlow College monitor the performance of key business applications to ensure they meet service level agreements (SLAs) and deliver a satisfactory user experience. This includes monitoring response times, transaction rates, and error rates.

4. Database Systems: Monitoring database systems involves tracking database performance, query execution times, storage usage, and overall database health. Carlow College ensure the reliability and efficiency of our databases to support business operations.

5. Security Monitoring: Carlow College employ robust security monitoring tools to detect and respond to security incidents in real-time. This includes monitoring for suspicious network activity, unauthorised access attempts, malware infections, and compliance with security policies.

Carlow College monitoring efforts are supported by a range of in-built and advanced tools and technologies that provide real-time insights into the health and performance of our IT environment. The College will configure alerts and notifications to promptly notify our team(s) of any anomalies or potential issues, allowing us to take proactive measures to address them before they escalate.

Regular reviews and analysis of monitoring data help us identify performance trends, optimise resource allocation, and plan for future technology investments. Carlow College hopes to maintain detailed documentation of monitoring configurations, incidents, and resolutions to facilitate transparency, accountability, and continuous improvement.

Overall, the College’s approach to monitoring the IT environment is proactive, agile, and aligned with the College’s goals and priorities. By leveraging advanced monitoring tools and best practices, Carlow College will ensure the reliability, security, and efficiency of our IT infrastructure to support the College’s mission and objectives.