CARLOW COLLEGE
ST. PATRICK'S

# TITLE: *INTERNET AND EMAIL USAGE POLICY*

| | | | |
|---|---|---|---|
| **Effective Date** | 20 March 2019 | **Version** | 01 |
| **Approved By** | Management Board | **Date Approved** | 20 March 2019 |
| | | **Review Date** | 20 March 2022 *or as required* |
| **Superseded or Obsolete Policy / Procedure(s)** | | **Owner** | |
| | | IT Services | |

## 1. Purpose of Policy

The *Email and Internet Usage Policy* has been developed to outline appropriate use of Carlow College, St. Patrick's (hereafter Carlow College) email system and internet communication systems and to provide staff and learners with details of what is deemed acceptable and unacceptable use of these systems. The purpose of the policy is to provide a safe, legal and appropriate manner for electronic mail communication and use of internet services within the College.[1] The policy also aims to eliminate potential risk to information security through inappropriate use of the email system.

By using the email and internet communication systems, all users with access to the Carlow College systems are agreeing to accept the terms of this Policy.

## 2. Definitions

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

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

*Intellectual Property* the intangible property that is the result of creativity, such as patents and copyrights (e.g. books, journals and movies).

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

*Network Security* is the protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system.

[1] The *Internet and Email Usage Policy* complies with the: *Prohibition of incitement to Hatred Act* (1989); *Criminal Damage Act* (1991) and the *Child Trafficking and Pornography Act* (1998).

## 3. Scope of Policy

This Policy applies to:

- all email communication services provided by Carlow College;
- all staff, agency staff, learners and third-party contractors of Carlow College with authorised access to the college email system and internet servicers, operating on behalf of the College; and
- all technology devices and resources provided by Carlow College IT Services including all connections to the network and internet both locally and remotely.

## 4. Policy Statement

Carlow College has a responsibility to ensure effective and appropriate use of its email and internet systems. All users of the email system are responsible and accountable for their use of electronic mail within Carlow College. The College understands its responsibilities to ensure the security of all internet and email systems by mitigating any vulnerabilities that may compromise the availability, confidentiality or integrity of its email and internet communication systems. The principles which underpin the use of Carlow College email system are:

- access to the Carlow College email facilities is regarded as a necessary requirement for business operations and no other purpose; and
- users have a responsibility to use facilities in an ethical and lawful manner and also in line with data records management, the *Data Protection Policy* and *Email Usage Guidelines* (Appendix 1).

### *4.1: Email Monitoring*

Carlow College reserves the right to log and record all email traffic within the college network and monitor routinely for the purpose of:

- troubleshooting technical faults and maintaining satisfactory system performance;
- maintaining system security on the email and college network ensuring confidentiality, availability and integrity of information stored on Carlow College network;
- preventing, detecting, inspecting and minimising inappropriate use of email facilities;
- ensuring compliance with Carlow College policies;
- monitoring will be carried out by IT Services Office or Line Managers, and monitoring will be carried out in compliance with *Data Protection Policy* and associated documentation; and
- retention of monitoring logs will be held in line with the *Records Management Policy* and the *Data Protection Policy*.

The College reserves the right on decision making as to whether the logs may be warranted for use in an investigation that may be linked to a disciplinary scenario.

*4.2: Personal Use of Email*

Email and internet facilities provided by Carlow College should be primarily used for daily business operations. However, occasional personal use may be permitted when:

- it does not cause financial or reputational damage to Carlow College, nor does it incur expense or liability for the College;
- all email and internet use are carried out in and ethical and legal manner in line with other college policies and associated documentation as listed in under section 5 and 6 of this document;
- is not excessive and does not take priority over college work responsibilities;
- the College holds the decision on what is considered excessive and any breach of this Policy and any breach or contravention of the policy may result in disciplinary action; and
- personal emails must be kept in a separate folder to college emails and personal sent items folder kept to a minimum.

*4.3: Transferring of Information and Records through Electronic Communications*

- All email communications should be sent in accordance with the guidelines set out in the *Information and Records Keeping Manual*, *Information Security Policy* and the *Data Protection Policy*.
- Senders of all electronic communications are responsible for the security and confidentiality of information they send.
- Access to shared mailboxes for circulating electronic communications will be granted based on role required and in line with access management and guidelines.
- Electronic communications containing college information which are sent or received on behalf of the college must only be sent through college email facilities and email accounts. The use of third party or private email accounts is strictly forbidden for the transfer or communication of college data.
- Confidential emails which are received via Carlow College email accounts must not be forwarded to personal accounts for security reasons
- Confidential or personal information which is received in an email should not be stored in a mailbox and should be saved and stored in line with the *Records Management Policy*.

*4.4: Shared Mailbox Access*

- In the case of operational requirement, a request can be made to IT Services by line management for the creation of a generic group mailbox. Access will be granted to users in line with *Access Management Policy* and group members will be included in group on line manager's instruction.
- Where generic email address is required (e.g. function@carlowcollege.ie), this will be appointed at the direction of line management.

- Users requiring access to their mailboxes or calendars must do so through granting system permissions rather than distributing their usernames and password.
- To ensure business continuity in the case of an absence and where the need is warranted, line managers may be permitted to access a colleague's computer for access to important college related information. This access will be granted at the discretion of management in substantial conditions that warrant doing so and only the required information being sought should be accessed in these circumstances.

### *4.5: Internet Access*

Access to Carlow College internet services is granted primarily to facilitate daily college operations, research, information sharing and communication. All users are accountable and responsible for their use of internet within the Carlow College network and will be granted access on the following basis:

- internet is used in an ethical and legal manner aligning with all other college policies and associated documentation and legal acts. Suspected illegal activity of internet usage may be reported to the Gardaí;
- all content accessed on the internet does not cause any harm, reputable damage, financial loss or legal implications to the College; and
- users accessing the college internet through personal/mobile devices are exempt from normal content filtering procedure, however are still responsible and accountable for all internet content access on their device through college internet and must ensure internet is used in accordance with all college policies and associated documentation.

### *4.5.1: Content Filtering and Traffic Monitoring*

Content filtering is applied on Carlow College network firewall to prohibit access to websites deemed inappropriate or unrelated to the daily operations of the College. Monitoring is also a critical part of supporting information security within the college. Content filtering logs will be monitored to:

- prohibit unauthorised downloading of software or non-college related programs without authorisation;
- the prevention of copyright infringement;
- prohibit excessive use of bandwidth through internet use;
- prohibit access to unlicensed software for which the College are not currently registered;
- detect anomalies in network traffic indicating adversarial risk to network services; and
- detect patterns of inappropriate use of internet services from specific IP network addresses, identifiable devices and usernames.

### *4.6: Unacceptable Use*

Carlow College internet and email services may not be used for:

- any activity that infringes rights on intellectual property of copyright;

- sending communications containing libellous, bullying, defamatory or illegal content or images;
- hacking, unauthorised email access or phishing purposes;
- any activity that may cause a security vulnerability for the College either deliberate or accidental;
- any action that may compromise network security within Carlow College;
- to generate, download, view or transmit any content of pornographic or sexual nature or that may be deemed inappropriate, discriminative or offensive to others; and
- for non-college commercial purposes that leads to non-organisational profit.

Carlow College holds the right to decide what is deemed unacceptable use of internet services.

## 5 Roles and Responsibilities

To ensure appropriate use of email and internet technologies within Carlow College, responsibilities lie under the following areas:

### *5.1: IT Services*

- Regular firewall auditing to ensure rules and settings are continuously updated and correct to ensure appropriate content filtering in place and low vulnerability to security through internet hacks.
- Ensure email addresses and internet facilities are secure and reliable
- Guaranteeing operations are carried out in line with Information security policy to ensure confidentiality, availability and integrity of email and internet facilities within the College.
- Generate awareness of information security while using internet and email facilities among staff.

### *5.2: Data Owners & Line Managers*

Data owners are responsible for:

- ensuring this policy and associated documentation are implemented in the areas for which they own data which may be used with email and internet facilities;
- making sure adequate procedures are in place to ensure awareness of security among staff in their area while using email and internet facilities;
- providing training if / when required to ensure staff in their area understand and comply with this Policy; and
- reporting any suspected misuse of internet or email facilities to the Data Protection Officer or IT Manager in line with the *Data Protection Policy*, *Internet and Email Usage Policy* and all other associated policies and documentation.

### *5.3: Users*

Each user who has been granted access to internet facilities and been assigned a carlowcollege.ie email address is responsible for:

- complying with this policy, associated policies and documentation;
- reporting any breach or misuse of college systems; and
- using internet and email facilities respectfully, ethically and in line with their college work and research.

## 6. Associated Documentation

- Appendix 1: Email Usage Guidelines

## 7. Referenced Policies

The following policies should be read in conjunction with the *Internet and Email Usage Policy*:

- *Information Security Policy*
- *Data Protection Policy*
- *IT Policy*
- *Access Management Policy*
- *Disciplinary Policy* (Staff)
- *Communications Policy*
- *Learner Code of Conduct and Disciplinary Policy*
- *Records Management Policy*
- *Remote Working Policy*
- *Social Networking and Social Media Policy*
- *Grievance Policy*

A number of other policies are currently in development which will be released through the quality assurance process to support (and in conjunction with) this Policy. All employees should ensure to keep abreast of policy developments within the College and speak with their Line Managers, Quality Assurance, or Human Resources should they have any questions.

The College reserves the right to amend these policies subject to organisational changes.

## 8. Monitoring and Review

A review of this Policy will be carried out bi-annually or as deemed necessary to organisation structural changes and also to ensure business needs are provided for and reflected in this policy. IT Services will work closely with the Data Protection Office to ensure any suspected breaches or changes to ensure security information within email and internet services can be mitigated and accommodated in this policy review.

**Appendix 1: Email Usage Guidelines**

CARLOW
COLLEGE
ST. PATRICK'S

## Email Usage Guidelines

The following are guidelines that must be followed when using the Carlow College email system:

1. ensure the account from which you are composing your email is your college account represented by professional email address and relevant display name;
2. ensure your email signature is correct and provides details reflecting your positions and contact information;
3. when using the "reply all" option to an email, ensure that replying to all recipients is warranted, appropriate and requires all included recipients to receive your response;

   proofread every message to ensure it is portrayed in the context for which it is intended and reads in that same context. Something that is perceived in a particular way when spoken may not come across in the same context when written in email;
4. when composing an email always be respectful of the recipient for which it is intended in terms of tone and content;
5. emails contacting passwords or personal information should be protected through password security or encryption;
6. when opening emails received, be aware of suspect or malicious emails which may be potentially harmful to your network. If something does not look genuine it most likely is not. In this case, move to your junk folder immediately;
7. ensure good housekeeping is regularly carried out on your mailbox by categories emails you are required to keep and removing emails which are unnecessarily taking up space in your mailbox;
8. use constructive subject lines to provide good indication to recipient of content of email;
9. when forwarding emails or message threads, ensure all recipients are warranted and justified in receiving the information. As stated in college policies and documentation, never forward emails containing personal information or information that is not relevant to the recipient; and
10. when sending/receiving email attachments, please consider the following:
    a. do not send large files through email as they will only clog up the mail server;
    b. limit the number of attachments sent in any one email;
    c. DO NOT open attachments which are received in emails from an unknown sender; and
    d. be conscious of sending attachments in a readable format. Do not send attachments in a format in which the recipient is unable to access the content.