# WEST COAST DISTRICT MUNICIPALITY

# Internet and E-mail Policy

Council Resolution: **ITEM 22/08/24/9.1.6**

# INTERNET AND E-MAIL POLICY

## 1. Policy overview

This Internet and email usage policy is designed to help you understand Council's expectations for the effective use of resources in the particular conditions of the Internet environment. The Internet and email facilities for West Coast District Municipality, hereafter referred to as Council, is a business tool, provided to you at significant cost to:

1. Use your Internet and email access for business related and/or educational purposes;
2. Conduct yourself honestly within existing Council Policies;
3. Respect Copyrights, Software licensing rules and Property rights.

(i) Unnecessary or unauthorized Internet and email usage causes network and server congestion. Unlawful Internet and email usage may also garner negative publicity for Council and exposes the council to significant legal liabilities.

(ii) Users must take special care to maintain the clarity, consistency and integrity of Council's corporate image and posture.

(iii) Internet and email also opens the door to some significant risks to our data and systems if we do not follow appropriate security discipline.

(iv) All employees granted Internet and email access with Council facilities will be provided with a written copy of this policy and must sign the attached declaration; opting not to sign will be seen as not being in need of these facilities, where after all access rights will be terminated.

## 2. Management and Administration

(i) Council has software and systems in place that monitor and record all Internet and email usage. Although the Internet and email usage won't be monitored by a member of the IT Committee on a daily basis, no employee should have expectations of privacy as to his or her Internet and email usage.

(ii) Management reserves the right to inspect any and all files stored in public and private areas of our network in order to assure compliance with this policy.

(iii) Internet facilities and computing resources must not be used to knowingly violate the laws and regulations of South Africa or the applicable laws and regulations of international bodies or governments.

(iv) No employee may use Council facilities to knowingly download or to distribute pirated software or data, or to deliberately propagate any virus, worm, Trojan horse, or trapdoor program code or to knowingly disable or overload any computer system or network, or to circumvent any systems intended to protect the privacy or security of another user or institution.

(v) No employee shall distribute the email address list of Council to a third party for marketing and/or advertising purposes, nor may it be used for chain mail or offensive marketing.

(vi) No employee, other than the Municipal Manager or officials who are duly authorized by him, may speak, or write and/or sign documents, on behalf of Council. Employees may participate in newsgroups or chat forums in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves, unless otherwise authorised to speak on behalf of Council.

(vii) Employees are reminded that chat and newsgroups are public forums where it is inappropriate to reveal confidential Council information, customer data, trade secrets or any other material covered by existing Council secrecy policies and procedures.

(viii) The Council will limit Internet access to all computer users.

(ix) It is a violation of Council policy to store, view, and print or redistribute any sensitive document or graphic file that is not directly related to the user's function or Council's business activities.

(x) Private email messages may be received and sent by users, but should be kept to an absolute minimum and should not include massive data, graphics or media files.

(xi) Misuse of the Internet and email facilities may lead to permanent disconnection of an user by order of management and may result in disciplinary steps against such an employee.

(xii) Employees may use their Internet and email facilities for non-business research or browsing during mealtimes, tea-breaks or outside of working hours, unless otherwise authorized, provided that all other Council policies are adhered to.

(xiii) Employees with Internet and email access may only download software, with written authorization of the IT Manager, for direct business purposes and must arrange to have such software properly licensed and registered.

Downloaded software may only be used under the terms of the relevant license agreements.

(xiv) Employees with Internet and email access may not use Council Internet facilities to download entertainment software or games, nor to play games against opponents over the Internet or network.

(xv) Employees with Internet and email access may not use Council Internet facilities to download videos, presentations or audio(music), unless there is an explicit business related use for the material. Employees with Internet access may not listen to radio or television channels over the Internet.

(xvi) Employees with Internet and email access may not upload or email any software licensed to Council, or data owned or licensed by Council, without explicit written authorization from the responsible member of the IT Committee for the software and data integrity of Council for that department.

(xvii) Employees with Internet and/or email access may not distribute data that may be termed offensive, nor may they visit websites which could be construed as being offensive.

## 3. Technical

(i) User ID's and passwords help maintain individual accountability for Internet and email resource usage. Any employee who obtains a password or ID for an Internet and email resource must keep that password confidential and private.

(ii) Employees should schedule communication-intensive operations such as large file transfers, video downloads, mass mailings and the likes for off-peak times. Large files must be compressed before sending or receiving.

(iii) Any file that is downloaded must be scanned for viruses, worms, Trojan Horses and trapdoor computer code or any other malicious content before it is opened/executed on a computer or in memory.

(iv) Video and audio downloading should be avoided.

## 4. Security

(i) A firewall has been installed for screening programs and other security systems to assure the safety and security of Council networks. Any employee who attempts to disable, defeat or circumvent any security facility will be subject to a disciplinary hearing.

(ii) File encryption must be used for secret and confidential documents sent and received over the Internet.

## 5. Creating reliable e-mail records

### 5.1 Structuring an out-going e-mail

5.1.1 E-mails that are public records shall contain sufficient information to ensure that they are properly contextualized and that they are meaningful and accessible over time.

5.1.2 Outgoing mail shall include the reference number of the subject folder in the file plan in the top right hand corner of the message box to provide a contextual link to the business activity that supports the e-mail.

### 5.2 Proper subject line

5.2.1 Subject lines are very important, since they indicate to a recipient what the message is all about.
If subject lines are not used appropriately, the recipients may not realize the importance of the message and choose to read it later or not at all. Users shall allocate useful subject lines to e- mails.

5.2.2 If a user receives a message with a senseless subject line and needs to reply to or forward it, the subject line should be changed to properly cover the subject of the e-mail before sending it off.

### 5.3 Auto-signatures

5.3.1 Staff should always be contactable even if their e-mail systems are down. Auto-signatures shall be used and shall contain the following identifying information of a sender:

- Name of sender
- Position of sender
- Name of unit/section
- Name of the governmental body
- Postal address
- Phone number
- Fax number

### 5.4 Attachments

5.4.1 If an outgoing mail includes an attachment, the attachment shall be filed into the file plan in the Integrated Document and Records Management System before it is attached to the e-mail to ensure that it contains the following prescribed minimum mandatory metadata.

- File plan reference number
- Record title: A sensible name given to it by the user
- Author
- Originating organization
- Originating sub office

5.4.2 Attachments shall be virus free.

## 6. Language used in e-mails

6.1 Official communications shall be approached in the same manner as a business letter, thinking it through carefully and using proper grammar and correct spelling.

## 7. Archiving

7.1 Work related email to a sender should be archived in the Document Management System (Collaborator).
7.2 The recipient is responsible for filing it.
7.3 E-mails considered to be public records shall not be deleted or otherwise disposed of without a written disposal authority issued by the National Archivist.