



Molemole Municipality

IT-01-01 INTERNET USAGE POLICY

Document Name: ICT Policy Framework

Policy Number: IT-01-01

Version: V001

Document Information

Policy	Internet Use Policy
Version	001
Policy Code	IT-03-05
File Name	POL-IT-03-05-004 Internet Use Policy.doc
Manual	IT Policies and Procedures Manual
Section	Information and Communication Technology
Applicability	This is applicable to all users of the Internet by users who use the Molemole Municipality Network infrastructure or computing equipment.
Situations	This applies in all situations in which a user gains access to the Internet.
Policy Owner	IT Manager
Policy Enforcer	IT Manager

1. Overview

1.1. General Purpose

Information and information resources are valuable assets of Molemole Municipality and they form an important part of the operation and management of the municipality.

This and other policies have been put into place in order to protect these and to promote integrity, security, reliability and privacy of the entire information infrastructure including the information and data it contains, the network, the computers and other access devices.

1.2. Background to this Policy

The Internet, and in particular the World-Wide Web, is a valuable resource for interacting and sharing information, as well as to retrieve information. The information potential of the Internet is virtually limitless with new paradigms emerging every year, such as the modern usage of the Internet for social networking, and the hosting of virtual meetings and conferences.

The usage of the Internet involves costs of bandwidth, as well as the usage of otherwise productive personnel time. There is an important requirement of the users to ensure that all usage of the Internet is done in order to improve the productivity of the user in meeting the goals of the municipality.

The implementation of this policy will provide a definition of the fine line between acceptable and unacceptable use of the Internet. This will benefit the municipality in allowing for informed self-discipline as the means for acceptable use.

2. Scope

This policy covers all usage of the Internet within the Molemole Municipality including the Web and all other forms of Internet usage.

Email is covered in a separate policy (Email Use Policy 03-01).

All users of the Internet are required to understand this policy and to apply this in their usage of the Internet at all times and in all situations.

This Internet Use Policy is related to the following Policies:

- 02-01 : Acceptable Use Policy

- 03-01 : Email Use Policy
- 04-03 : Information Sensitivity Policy
- 05-06 : Information and Network Security Policy

3. Purpose of this Policy

- 3.1. The purpose of this policy is to ensure that access to the Internet by users is conducted appropriately as well as to define the difference between acceptable and unacceptable use.

4. Applicability

- 4.1. This Policy is applicable to all usage of the Internet facilities provided by the municipality.
- 4.2. This policy may also be applicable to public users of municipal services, such as individuals that make use of computer facilities in libraries and Internet cafés which have access to the Internet.

5. Definitions for this Policy

- 5.1. **Audio Streaming / Video Streaming, Media Streaming:** The sending of receiving of live feeds of data for audio, video or other media, which are converted into audio or video on the client workstation by means of a media player.
- 5.2. **Discussion Groups :** these consist of all types of online discussions conducted over the Internet.
- 5.3. **Firewall :** Software located on servers that connected to the Internet that allow for control over the nature of the information transfer into and out of the servers. These are primarily used to protect servers and the users of the servers from malicious software.
- 5.4. **Internet Chat Rooms :** A communal facility on the Internet in which groups of people are able to chat by text, voice or video.
- 5.5. **Internet Infrastructure :** This refers to the Molemole Municipality Internet Infrastructure including access to Internet, routers and switches for networking, the entire network, all workstations and all information facilities and content stored on Internet sites managed by the municipality.
- 5.6. **ISP :** Internet Service Provider.

- 5.7. **MFMA** : Municipal Finance Management Act.
- 5.8. **Monitor**: includes the terms monitor, inspect, copy, review, store.
- 5.9. **Social Networking Sites** : These include web sites such as YouTube, Twitter and Facebook and all similar sites.
- 5.10. **Users** : The term “user” applies to all users of computers within the scope of the municipality, whether these users are connected to the municipal network or not and will apply to employees, contractors, consultants, part-time staff, temporary staff, and any other workers who bring their computers into the municipality or who have access to the computing equipment, networks and information resources of the municipality.
- 5.11. **Viruses** : The term “virus” is used as a generic terms to cover various threats to computing facilities which include viruses, worms, email bombs, trojan horses, phishing, and all related programs which provide some level of disruption of services. At worst these programs result in total loss of the information services. At best they be a minor inconvenience resulting in loss of time and cause reduction in efficiency of effectiveness of the information services.
- 5.12. **Web Sites** : A server that runs a web server system and which provides access to information over the HTTP Protocol via Web Browsers.

6. Policy Statements

Internet Access

- 6.1. Users are granted access to the Internet as required for their specific job responsibilities.
- 6.2. The allocation of Internet access rights is required to be approved by the next level manager and by the IT Manager.
- 6.3. Internet access rights may be specified within specific restricted web sites and facilities only.
- 6.4. There is no automatic access to the Internet, and this is not a right of the user. Misuse or abuse of the Internet facilities will lead to revoke of the privilege and the potential for disciplinary action as per the enforcement section of this policy.

- 6.5. Only workstations specifically identified by the IT Help Desk and/or specific user accounts will be authorised to be connected to the Internet Services.
- 6.6. Access to the Internet Services via remote services such as dial-up and VPN are allowable within the provisions of the Information and Network Security Policy (05-06).

Online Communication and Virtual Meetings

- 6.7. The primary benefit of Internet Access to users is to enable the users to obtain relevant information to assist them in carrying out their work for the municipality.
- 6.8. Another important business benefit is to facilitate inter-communication between the municipal officials, employees and partners beyond the limited capabilities of Email as a means of communication.
- 6.9. This type of Internet usage is encouraged and includes online communities of practice and virtual meetings. The usage of these facilities helps to make the municipality more effective and efficient.
- 6.10. When meetings are held via Instant Messaging applications or Virtual Meeting technologies these should be logged and the logs retained as the formal records of the meetings.

Monitoring of Internet Usage

- 6.11. The provision of an Internet Service to users which provides access to Web Sites and other services does not imply permission has been granted to access all Internet Services. The Internet is an open information space and this policy statement outlines the rules of acceptable usage which should guide the user in self-management of their behaviour when using this privileged service.
- 6.12. All users are monitored in terms of their usage of the Internet. This includes specifically the Web Sites and other Internet Services that are used including online time and bandwidth usage.
- 6.13. When it is suspected that a user may have been misusing the Internet, the IT Manager will identify a particular person to review the suspected misuse, and this person may then gain access to the same web sites in order to determine whether these are infringements or not, and to produce a report on this monitoring activity including all web sites visited and recommending whether they should be placed onto the banned list

of web sites. No other access to such sites is permitted by anyone in the normal course of their work.

- 6.14. The usage will be produced as a report on a monthly basis and provided to the manager of the SBU as well as to the user for every user who is granted Internet access.
- 6.15. The largest users in terms of resources such as bandwidth are always reviewed monthly.
- 6.16. Specific Web Sites will be blocked by the Firewall in order to prevent access to those Web Sites deemed unsuitable for productive usage of the Internet Services. This list will be maintained by the IT Help Desk and will up updated regularly.

Internet Chat / Newsgroups / Discussion Groups

- 6.17. Usage of Internet Chat Rooms, Newsgroups, Discussion Groups, Social Networking sites and all similar activities is expressly forbidden in terms of this policy. If there is case for this to be used as part of the municipal communications policy then this restriction can be relaxed on a case by case basis.
- 6.18. When a user uses an Internet Chat room, a newsgroup or any discussion group on the Internet they are required to indicate a message clearly indicating that their comments are personal and do not reflect the position of the Molemole Municipality.

Media Streaming

- 6.19. Usage of all media streaming sites and facilities on Web Sites is expressly forbidden for non-business purposes. The usage of such facilities greatly impedes the capacity of the municipal Internet connection and causes a loss of productivity for all users of the Internet Services.

Instant Messaging Applications

- 6.20. Instant messaging applications, such as Skype and Yahoo Messenger are restricted from usage for all users under normal conditions.
- 6.21. Each user must make a specific request to open up these Instance Messaging Services by a request to the IT Manager, motivating this usage.

Posting to Internet Services and Sites : Considering Information Rights

- 6.22. All users who post any data to any Internet site, whether this be a Web Site or any other Internet service, are required to obtain permission for this in advance from the Communications Manager and other managers as appropriate to the type of posting. The Communications Manager will receive input and support from the IS Department where appropriate.
- 6.23. Much of the data and information contained on the Internet is protected under various rights, including copyright, patents and trademarks. Consideration must be given to these rights whenever using information and data extracted from the Internet. The rights will be identified in terms of the Web Site usage disclaimers as well as other messages associated with particular files and web pages. In the absence of anything to the contrary, there will be residual author copyright in all information available over the Internet unless this is specifically identified as out of copyright.
- 6.24. When a user quotes from a specific Internet source it is essential that the citation indicated where this was obtained from and the date on which this was obtained.
- 6.25. A user should only repost information on the Internet with the permission of the rights owner.
- 6.26. A user should never post sensitive information on the Internet in any form.

Unacceptable Usage

- 6.27. The following situations of Internet and Intranet usage are specifically prohibited, as well as any situation that are similar in spirit to these stated situations but are not necessarily limited to the situations discussed below. These specifically apply to situations in which the user is using a Molemole user account or using Molemole networks or computing facilities or access via mobile phones or PDAs. This applies to both accessing of information and posting of information:
- Using the municipal Internet facilities to post political statements
 - Accessing pornography or obscene information in any form, including images, video and text.

- Posting any information that falls into a wide range of unacceptable content including : hate speech, abusive, defamatory, conflict, information to embarrass colleagues or others by information based upon any discriminatory practice including ethnic origin, age, gender, health, physical characteristics, religious persuasion, sexual orientation; any materials which contains sexual harassment content
- Personal advertisements
- Petitions
- Conducting personal business
- All activities that would be considered illegal if conducted in any other manner

Leisure Time vs Work Time

- 6.28. There is no difference in the application of this policy between working hours and after-hours time including lunchtimes, since at all times Internet usage incurs costs to the municipality. The Internet Services are assets of the municipality and are required to be used efficiently and effectively in order to accomplish the goals of the municipality as identified in the MFMA.

Monitoring of Internet Usage

- 6.29. All Internet access will be monitored at all times in terms of usage and web sites visited and non-web facilities used (for example Sykpe, Second Life).
- 6.30. On a regular basis all users will receive a list of their Internet usage and be asked to confirm their usage of facilities and sites which are outside of standard authorised sites.

7. Procedure : Granting/Limiting/Revoking Access to the Internet

Trigger

- 7.1. This is triggered by a request from a user of the information services to be provided with access to the Internet.

Requester

- 7.2. Any user of the municipal information services can request access to the Internet.

Responsibility

- 7.3. This is the responsibility of the Network Manager, and each request is required to be authorized by the IT Manager.

Steps

Seq	Activity	Who	Duration
1	User requests access to the Internet using Form 05-56 : Request for Internet Access	Requester	
2	Form is provided to Admin Officer who checks the details and ensures that the Requester understands the Internet Use Policy and other related policies. The form is passed onto IT Manager for approval.	Admin Officer	1 day
3	Application is approved or rejected. Rejections require an explanation to be provided.	IT Manager	2 days
4	Rejected applications are sent back to the requester.	Admin Officer	
5	Approved applications are submitted to the Network Manager	Network Manager	
6	User is provided with Internet Access with certain limitations as required.	Network Manager	
7	Form is returned to Admin Officer for filing.	Admin Manager	

Forms

- 7.4. Form 05-56 : Request for Internet Access which must have the following fields:

- Details of requester
- Reason for needing Internet access – in particular why this is relevant to the work responsibilities
- How much access is required
- Specific sites that the requester needs to access.
- Signatures of IT Manager, SBU Manager and requester.

Enforcement

- 7.5. This is enforced by the IT Manager.
- 7.6. The nature of the enforcement is dependent upon the nature and severity of the violation of this policy.

8. Procedure : Monitoring and Reporting on Internet Usage

Trigger

- 8.1. Regular monthly reports on usage.
- 8.2. Ad hoc monitoring concerning specific users in cases in which there is initial suspicion of misuse that is required to be confirmed

Requester

- 8.3. IT Manager.

Responsibility

- 8.4. This is carried out by the Network Manager.

Steps

Seq	Activity	Who	Duration
1	Extract the history of Internet Usage in terms of web sites visited, dates, and bandwidth used for the selected users.	Network Manager	
2	Summarise this in terms of specific web sites which are suspected as being outside of the policy.	Network Manager	
3	Report to the IT Manager for action and decision.	IT Manager	
4	Produce a monthly report on the largest users of the Internet, indicating the web sites that they have visited.	Network Manager	
5	Email the largest users with a warning to cut down their usage if this is not for municipal purposes.	IT Manager	
6	Identify web sites which need tighter control and restrict these through the firewall facilities.	Network Manager	
7	Any serious transgressions of this policy must be identified and passed on to the HR department for disciplinary action.	IT Manager	

9. Forms / Registers

- 9.1. Request for Internet Access (05-56)

10. Enforcement

- 10.1. Transgressions of this Internet Use Policy will be inter alia dealt with in terms of the Municipality's Disciplinary Code and Labour Legislation. Non-employees will be prosecuted under applicable legislation of the RSA.
- 10.2. A transgression may result in the permanent or temporary removal of access to the Internet System and to other information services, computing services and computer equipment.

11. Review and Audit

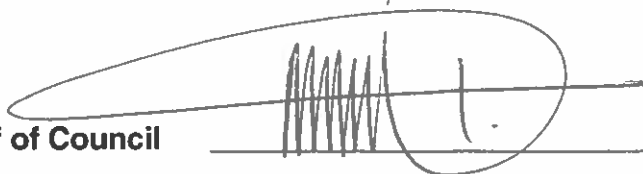
- 11.1. This policy will be reviewed in accordance with the ICT Policy Framework.
- 11.2. The enforcement of this policy will be audited as follows:
- Regular monitoring of Internet usage by individual user.
 - Interviews with transgressors.

*** END OF DOCUMENT ***

a) Date of Approval by Council

29/05/2025

b) Signed on behalf of Council

A large, stylized handwritten signature in black ink, consisting of many vertical strokes and a large loop, is written over a horizontal line.