

RAMOTSHERE MOILOA LOCAL MUNCIPALITY

INTERNET ACCEPTABLE USE POLICY



Introduction.....	3
Background.....	3
Objectives of this Policy.....	3
Application of this Policy.....	4
References and Related Legislation and Regulations.....	4
Policy Statement.....	4
Methods of Connecting to the Internet.....	4
Detection of Viruses.....	5
External Email accounts and Instant Messaging.....	5
Distribution of Information and Data.....	5
Communication of Official Information.....	5
Discussion Groups.....	6
Copyright Restrictions.....	6
Frivolous Use.....	6
Limitation of Privacy.....	6
Discriminatory, harassing and/or offensive language.....	6
Installation and Downloading of Software.....	7
Additional Connections to the Internet.....	7
Monitoring and Reporting.....	7
Prohibited Use.....	8
Conditions for internet Access.....	8
Authorization Procedures.....	8
Internet User's Responsibilities.....	9
Consequences of Non-Compliance.....	9
Appendices	
Annexure A – Terms and Abbreviations	
Annexure B – Internet User Undertaking Form	

1. Introduction

The World Wide Web is a worldwide network of computers that contains millions of pages of information. The internet is a necessary job-enhancing tool because it allows internet users access to information required to carry out and enhance their jobs when required. Recognising the importance of the internet, many organisations and government departments have implemented information systems to provide staff members with access to the internet.

However, an organisation which connects its networks to the internet exposes its information systems to all kinds of internet-borne security risks due to the open nature of the internet. Furthermore, current-day applications like e-mail, www, etc require relatively large amounts of bandwidth, of which the demand and cost is very high.

As a result organisations connected to the internet need to implement technical and procedural measures to mitigate risks from untrusted networks and to ensure that internet resources are utilized in a manner which does not adversely impact normal business operations.

2. Background

Ramotshere Moilola Local Municipality provides internet and World Wide Web access to all its employees and employees are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the internet.

Even harmless search requests may lead to web sites with highly offensive and/or malicious content. Additionally, having a web-based email account on the internet may lead to receipt of unsolicited e-mail containing offensive and malicious content.

While Ramotshere Moilola Local Municipality implements adequate measures to govern internet usage, employees are ultimately responsible for any internet-related activities and any material viewed or downloaded by users from the Internet. To minimize these risks, the use of the Internet facilities at Ramotshere Moilola Local Municipality is governed by this Internet Acceptable Use policy.

3. Objectives of this Policy

The objectives of this policy are:

- i) To define security "laws and governance" that shall be enforced departmental wide to ensure that Ramotshere Moilola Local Municipality internet information systems are adequately protected from misuse or direct/indirect exposure to security risks

ii) To ensure the highest possible level of Confidentiality, Availability, Reliability and Integrity for the Ramotshere Moiloa Local Municipality network, Information and information systems

iii) To encourage cost-effective and productive use of Ramotshere Moiloa Local Municipality internet systems

iv) To clearly define user responsibilities and liability when using departmental internet facilities in day-to-day activities

v) To ensure compliance with regulations of RSA and other relevant international laws, regulations, standards and best practices

4. Application of this policy

This policy applies to all employees (including service providers, contractors and temporary staff) utilizing departmental internet systems via 3G cards, departmental computers and laptops as well as Ramotshere Moiloa Local Municipality networks.

5. References and Related Legislation and Regulations

The following publications govern the execution of the internet use policy and were taken into consideration during the drafting of the internet use guidelines and policy:

- i) SABS/ISO 17799
- ii) Information Security Forum (The standard of good practice for Information Security)
- iii) Minimum Information Security Standards
- iv) Copyright Act
- v) Protection of Information act
- vi) Public Service Act
- vii) National Strategic Intelligence Act
- viii) Interception and Monitoring bill
- ix) Regulation of Interception of Communications Act
- x) COBIT Audit framework
- xi) Electronic Communications and Transactions Act
- xii) International Standard for Risk Assessment
- xiii) Ramotshere Moiloa Local Municipality formation Security Policy

6. Policy Statement

Internet users are expected to use Ramotshere Moiloa Local Municipality's internet facilities in a responsible manner which complies to the laws and regulations of RSA, other international laws as well as policies, standards and guidelines as set by Ramotshere Moiloa Local Municipality.

Access to Ramotshere Moiloa Local Municipality's internet facilities is a privilege that may be wholly or partially restricted by the department without prior notice and without the consent of the internet user when required by and consistent with the law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to Ramotshere Moiloa Local Municipality procedures or, in the absence of such procedures, to the approval of the I.T Office.

6.1 Methods of Connecting to the Internet

To ensure security and avoid the spread of viruses and other security threats, Users accessing the Internet through a computer attached to Ramotshere Moiloa Local Municipality 's network must do so through the departmental Internet proxy server or other information security systems like firewalls, Intrusion Prevention Systems, etc. Every employee will use his or her network username and password to access the internet for accountability and reporting purposes.

Bypassing Ramotshere Moiloa Local Municipality's computer network security by accessing the Internet directly by modem, 3G cards, and mobile phones connected to computers, non-Departmental wireless networks or other means is strictly prohibited unless the computer you are using is not connected to Ramotshere Moiloa Local Municipality network. Disabling of or subverting any security software installed on departmental computers shall also constitute breach of this policy.

6.2 Detection of Viruses

Files obtained from sources outside Ramotshere Moiloa Local Municipality, including fixed and/or removable disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by vendors, may contain security risks that may damage Ramotshere Moiloa Local Municipality's computer network.

Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non- Ramotshere Moiloa Local Municipality sources, without first scanning the material with Ramotshere Moiloa Local Municipality approved virus checking software.

If you suspect that a virus has been introduced into Ramotshere Moiloa Local Municipality's network, notify Ramotshere Moiloa Local Municipality I.T Office immediately. If you are uncertain how to scan for viruses immediately contact I.T Office for assistance.

6.3 External Email Accounts and Instant Messaging

While external web mail accounts are not disallowed, users must ensure that these email accounts are not used to distribute and/or store official information as this might lead to intentional/unintentional disclose of sensitive official information.

Only departmental email systems must be used when distributing official information. Due to high number of security risks associated with Instant Messaging applications line msn messenger, yahoo messenger, etc users are not allowed to use and install any instant messaging application on departmental computers or networks.

6.4 Distribution of information and data

Without prior written permission from Ramotshere Moiloa Local Municipality, the Ramotshere Moiloa Local Municipality's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, trojan horse programs, etc.) or any other unauthorized materials.

Occasional limited appropriate personal use of the computer is permitted if such use does not a) interfere with the users or any other employee's job performance;
b) Have an undue effect on the computer or Ramotshere Moiloa Local Municipality network's performance;

c) Or violate any other policies, provisions, guidelines or standards of this agreement or any other of Ramotshere Moiloa Local Municipality Further, at all times users are responsible for the professional, ethical and lawful use of the departmental internet facilities.

6.5 Communication of Official Information

Unless expressly authorized to do so, users are prohibited from sending, transmitting, or otherwise distributing official information, data or other sensitive/confidential information belonging to Ramotshere Moiloa Local Municipality through the World Wide Web.

Unauthorized dissemination of such material may result in severe disciplinary action and other appropriate actions under the laws and regulations of RSA or any international laws.

6.6 Discussion Groups

No Ramotshere Moiloa Local Municipality employee may in his/her official capacity create, participate in discussion groups on the internet without authorization from his or her manager.

6.7 Copyright Restrictions

Users may not illegally copy material protected under national and international copyright laws or distribute that material to other people. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy.

You may not under official duties agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the Department.

6.8 Frivolous Use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all internet users have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer/network resources or unfairly monopolize resources to the exclusion of others.

These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing online games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, accessing P2P networks/applications or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

6.9 Limitation of Privacy

Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should acknowledge and understand the openness and privacy issues relating to the internet and as such have no expectation of privacy in anything they store or distribute using the Ramotshere Moiloa Local Municipality's internet facilities.

User consents to allow authorized I.T personnel to access to and review of all materials created, stored, sent or received by User through departmental Internet facilities for the purposes of accounting, monitoring of policy compliance and internet usage statistics.

6.10 Discriminatory, harassing and/or offensive language

Users are to refrain from using obscene, defamatory, derogatory, discriminatory or any offensive language while using Ramotshere Moiloa Local Municipality's internet facilities as such actions could have serious criminal, civil and moral consequences.

6.11 Installation and Downloading of Software

Recognizing the many security risks on the internet, users are cautioned not to install or download any software from the internet as this might result in copyright violations, virus infections, and installation of adware, spyware and malicious monitoring software.

Opening malicious web sites can often lead to automatic installation of malicious software and users are also cautioned not to agree to any automatic installation presented by web sites. If a user is uncertain about how to proceed, it is his or her responsibility to get advice from I.T Office. A user knowingly downloads and installs any software from the internet that can compromise the Ramotshere Moiloa Local Municipality network, information systems or other users will be in violation of this policy.

6.12 Additional Connections to the Internet

The department offers additional tools like 3G cards to selected employees to help enable remote internet connection and access to emails from remote locations. It must be understood that the usage of these 3G cards are governed by this Internet Acceptable Use Policy and as such 3G users must ensure that they utilize these 3G cards for official purposes.

3G users are more vulnerable to virus attacks and other security risks from the internet as they are not protected by departmental information security systems. This means that a 3G user visiting malicious sites could unknowingly distribute security risks to other computers while connected to the Ramotshere Moiloa Local Municipality Network.

No internet user is allowed to configure or enable other connections to the internet via modems, wireless networks and cell phones on departmental computers. Any additional internet connections should be reported to I.T Office.

6.13 Monitoring and Reporting

Ramotshere Moiloa Local Municipality accepts that the use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the Department. In addition, all of the department's Internet facilities are provided for primarily official purposes.

Therefore, the Department maintains the right to monitor and log the volume of Internet and network traffic, including but not limited to Internet sites visited, files downloaded by users, etc. The specific content of any transactions will not be monitored unless there is a suspicion of improper use or policy violation. It may also be necessary for authorized I.T personnel to view the contents of employees' electronic communications and internet activity history in the course of problem resolution.

I.T support personnel may not view an employee's electronic communication out of curiosity or at the request of individuals who have not followed the correct authorization procedures. Furthermore internet activities will be logged for reporting/statistics purposes and provided occasionally or on demand to I.T management to enable proper implementation of systems that will cater for the future growth demands and to ensure on going availability, scalability and reliability of these systems.

7. Prohibited Use

7.1 Accessing streaming audio or video, play online games

7.2 Accessing chat sites

7.3 Installing and using instant messaging applications

7.4 Download of copyrighted material including videos, music, software or any intellectual property

- 7.5 Accessing web sites and material that may be offensive to other employees. This includes but not limited to pornography, hate speech web sites, criminal/illegal activities, etc
- 7.6 Using the internet to conduct criminal or fraudulent activities
- 7.7 Using the internet to illegally monitor, gather information about any individual, entity or organization.
- 7.8 Using the internet to intentionally subvert security systems or initiate a denial of service against any information system or network
- 7.9 Using the internet to conduct any personal business operations at the expense of the department's bandwidth and resources
- 7.10 Connecting to the internet via 3G while the computer or laptop is connected to the Departmental network.
- 7.11 Using the internet such that it interferes with employee productivity
- 7.12 Sharing of usernames and passwords used to access the internet with other people including employees
- 7.13 Distributing of passwords or any sensitive user account information through the internet
- 7.14 Impersonating, misrepresenting or suppressing a user's identity when accessing the internet
- 7.15 Using 3G cards for making telephone calls
- 7.16 Using the departmental internet facilities to intercept or disclose, or assist in intercepting or disclosing electronic data or information.
- 7.17 Accessing P2P networks and web sites
- 7.18 Using profanity, obscenities or derogatory, sexist, racist, highly sensitive, offensive or defamatory remarks while using the internet.
- 7.19 Using the internet to access malicious sites and download illegal material
- 7.20 Use of VoIP applications not necessary for official duties e.g. skype

8. Conditions for internet Access

An employee must sign and accept the conditions and liabilities of this internet acceptable use policy before being granted access to the network. If the internet user then violates any part of this policy, remedial actions such as revoking the user's internet access and/or disciplinary may be taken. Depending on the outcome of the investigations the user may be required to reapply for internet access by filling in the relevant forms.

9. Authorisation Procedures

For purposes of ensuring proper use accountability, control and proper use of the Internet, every employee utilizing a departmental notebook, computer, 3G card shall sign an undertaking in the format **Annexure B**, through which, he/she will abide by the policy stipulations contained in this policy.

This undertaking will be presented by I.T Office or the Personnel Office to the employee. The signed undertaking will be filled in the staff file of the employee. IT/Personnel Office will take all steps to ensure that all the employees are provided with these undertaking forms. Failure to sign shall lead to existing internet access for that employee revoked.

10. Internet User's Responsibilities

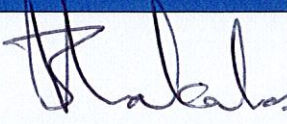
All internet users are responsible, accountable and liable for all their activities while browsing the internet. As such the internet user has the following responsibilities:

- a) Ensure that their usernames and passwords are kept secure and not shared
- b) Fully comply with all aspects of this policy
- c) Immediately alert I.T Office (Information Security/Incident Response) about any misuse and non-compliance.
- d) Duty not to waste computer/network resources
- e) Understand that the information or data sent via the internet may/can be intercepted by other individuals and ensure that they fully acknowledge this privacy concern.

11. Consequences of Non-Compliance

All Ramotshere Moiloa Local Municipality employees, contractors or temporary staff who have been granted the right to use the Ramotshere Moiloa Local Municipality's Internet access are required to sign this agreement confirming their understanding and acceptance of this policy.

All employees, contractors or temporary staff who have been granted the right to use the department's Internet facilities are required to sign the internet user undertaking confirming their understanding and acceptance of this policy. As already stated, on-compliance of this policy may lead to disciplinary actions, legal liability as well as internet privileges for the user in violation revoked.

DESIGNATION	NAME	SIGNATURE	DATE
ACTING MUNICIPAL MANAGER	Mr. T. PHAKALANE		30/05/2016

COUNCIL RESOLUTION

COUNCIL RESOLUTION NUMBER	DATE
59/05/2016	30 MAY 2016