OVERSTRAND MUNICIPALITY

ELECTRONIC COMMUNICATIONS POLICY

Amendment 1

Approved by Council

29 August 2012

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

This policy is applicable to all employees of the Municipality with access to a municipal owned or sponsored computer, software and network facilities which consequently may have access to electronic mail, online services and the Municipal Intranet.

The Municipality encourages business use of e-mail between staff and clients as communication is made more efficient and facilitates the business of the Municipality.

While respecting the privacy of its employees, the Municipality is also concerned with protecting and securing itself and its computerised information. The Municipality needs to maintain a high level of professionalism and therefore needs to monitor and manage the use of its resources in a manner that will maximise business operations.

Each employee should be aware that the Municipality and its Information Communication Technology (ICT) personnel, in the course of maintaining the Municipal systems and computer network, routinely monitor employee activities conducted on Municipal information systems and networks. If the Municipality or its ICT personnel discover evidence of misuse, illegal activity or any activity that violates any of the Municipal policies and rules, the Municipality may consider appropriate corrective action and/or disclosure of evidence to law enforcement officials.

The purpose of this policy is to define the rules of conduct and behaviour of all municipal employees and contract personnel (hereinafter collectively referred to as "user(s)" when utilising electronic mail, the Internet, secure dial-in or any other communication facility from This policy must be read in conjuction with the Municipality's ICT Information Security Policy.

1.2 Amendment 1

1.2.1. The purpose of this amendment 1 is to enable employees to make use of the municipal internet access services for study purposes in compliance with Municipal policies and regulatory requirements. A new paragraph 2.1.1.sub-paragraph d) has been formulated to give effect to this amendment.

1.2.2. It was also noted that the numbering for paragraph 2.1.3 a) to i) is incorrect. The first paragraph is an introductionary paragraph and the subsequent paragraphs are sub-paragraphs to the introductionary paragraph. The sub-paragraphs will be renumbered from a) to h) in this amendment 1.

2. POLICY

2.1 Use of the electronic communication facilities and services.

2.1.1 Primary use for Municipal business purposes

a) Employees are allowed access to communication facilities and services for bona fide Municipal business purposes. The use of such facilities may also be used for occasional and limited personal, non- business purposes. Non-business communications must in any event comply with the standards of communication set forth in the “Standards of Communication” section as well as all other provisions of this policy and will be treated as all other Municipal communications.

b) Certain users may be assigned Internet access where such access is essential to the performance of such user's duties at the Municipality.

c) Internet access as is necessary for research or other purposes must be approved in writing by the relevant Manager and submitted to the Manager: ICT.

d) Certain users may also be assigned Internet access where such access is required for study purposes, specifically for curriculums or study guides approved by the management in compliance with existing policies or regulatory frameworks, to improve their performance and/or career opportunities in the municipality. Internet access as necessary for studies and applicable research must be approved in writing by the relevant manager and submitted to the Manager IT. This internet access will only be for a limited period and such periods must be specified by the manager when approval is granted to an employee.

2.1.2. Standards of Communication

a) Each user has a responsibility to use the communication facilities and services in a lawful, informed and responsible way and in a manner that conforms to computer network etiquette, custom, courtesy and corporate policy.

b) Users must apply exactly the same standards of care and professionalism when using electronic communication facilities and services as they would apply in any other business related communications.

2.1.3. Prohibited Conduct

Examples of misconduct relating to computers, software and hardware, electronic mail, online services, the Internet and Municipal provided dial-in facility include, but are not limited to, the following:

a) use of electronic mail, online services, Internet facilities and Municipal secure dial-in Services for unlawful or malicious activities;

b) use of defamatory, abusive or objectionable language in either public or private Communication;

c) misrepresentation of oneself or inappropriate representation of the Municipality;

d) activities that cause congestion and disruption of the Municipality's networks and systems (e.g. large e-mail attachments, chain letters or graphics);

e) any attempts to compromise security on any Municipal system e.g. "hack" into systems or another person's log-in, "crack" passwords, breach computer or network security measures, or monitor electronic files or communications of other employees or third parties, except by the explicit direction of the Municipal Manager in accordance with paragraph 2.2 below;

f) use of electronic mail for communications that contain improper or unlawful statements including, but not limited to, ethnic slurs, racial epithets, religious solicitation or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, sexual orientation, age, disability or religious beliefs, or communications that contain sexually explicit or offensive images, cartoons, graphics, sound or text;

g) use of internet connectivity to view or transmit content which include, but is not limited to, ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, sexual orientation, age, disability or religious beliefs, or content of a sexually explicit or pornographic nature such as offensive images, cartoons, graphics, sound or text;

h) negligent misconduct in relation to computers and software technology which includes but is not limited to:

- willful or negligent introduction of a virus into a user's computer or any other computer system in the Municipality;
- intentional or grossly negligent damage to computer hardware or software belonging to the Municipality or an employee;
- spending unauthorised and/or excessive time on the Internet, e-mail or other Communications systems for non-business purposes;
- divulging of allocated user names and/or password to any third party or co-employee or allowing a co-employee or third party to use the user name and/or password;
- unauthorised use of an employee's terminal or a co-employee's terminal or other user's terminal;
- unauthorised use of private software on Municipal computers, or downloading and unauthorised copying of software for home and external use.

2.2. Monitoring of communication by the Municipality

The Municipality, in its discretion, reserves the right to monitor usage patterns for Internet communications and monitor and examine the contents of e-mail messages.

2.3. Security measures and limitations on access

a) Each user must comply with all of the Municipality's access procedures, including the use of assigned user ID's and use of the Municipal licensed software made available to the employee by the Municipality.

b) User IDs may not be shared with other persons, a user may not use e-mail accounts assigned to other individuals to send or retrieve messages.

c) It remains the responsibility of each user to safeguard their passwords to prevent unauthorised access. Users must ensure that system access is signed off when they leave their desks.

d) The user must contact the Department: Information Communication Technology immediately if his/her computer or any equipment is stolen to be able to cancel all network access for that user.

2.3.5. The Municipality also reserves the right to:

a) selectively restrict user access to certain hardware and software;

b) install security measures such as passwords and/or selectively restrict access to relevant parts of the network only;

c) disable access to certain Internet protocols such as Internet Relay Chat (e.g. mIRC) and Newsgroups;

d) install software to screen out access to undesirable web sites;

e) install software to track or monitor e-mail and/or Internet usage;

2.3.6. All users are expected to use good judgement when using the Internet. Users may not use the Municipality's name or property or a Municipal provided Internet ID to represent themselves as someone else. Use of the Internet reflects on the Municipality's reputation and legal responsibilities. Usage must reflect the Municipality's business goals, responsibilities or values.

2.3.7. All users must respect the intellectual property rights of the Municipality and third parties (patents, copyrights, trademarks and trade secrets).

2.4. Accessing the Internet to upload and/or communicate

2.4.1. E-mail usage

a) All correspondence sent over the Internet, such as e-mail, bulletin board notes and other messages must be treated as if they are public and printed on the Municipality's letterhead.

b) Users must observe the same standards when sending e-mails that apply when acting for the Municipality in normal written communications.

c) Communication via e-mail is, by its very nature, informal and hence impulsive. Caution must be observed when communicating via e-mail and drafts must be checked properly before being sent.

d) Users may not use the Municipality's name or any part thereof as part of a personal e-mail account, ID or non-municipal Web page in any non-municipal situation. Any e-mail sent or received on the Municipality's equipment is considered to be Municipal property.

e) Users may not distribute Virus warnings as many Virus warnings on the Internet are hoaxes and in some cases may cause more damage than an actual virus. If a user receives a Virus warning he/she must forward the message to the Department: Information Communication Technology. Only Virus warnings received from the ICT management must be considered authentic and Virus warnings from any other party must thus be ignored until confirmation is received from the Manager: ICT

2.4.2. Remote Access Through Dial-up Services

a) Remote access through dial-up services is subject to the same security principles and rules relating to computer hardware, software, network and any information system or service provided and/or sponsored by the Municipality.

b) Any computer or independent dial-up to any external computer or network must be physically isolated from the Municipality's internal networks. Use of a modem while connected to the Municipal network is an offence and the Municipality shall take appropriate corrective action against any person who does not observe this rule.

c) Remote Access to Municipal systems may only be implemented through the approved procedures

d) Remote dial-up User ID's may not be shared with other persons and a user may not use a dial-up account assigned to other individuals.

e) Users must notify the Manager: ICT immediately if they become aware of any situation that might compromise the security of data, systems and or equipment.

2.4.3. Internet Usage

a) Access to the Internet must be approved by management, and provided by the Department: Information Communication Technology.

b) Each user accessing Internet facilities of the Municipality shall identify himself or herself honestly, accurately and completely through the use of a standard Logon ID and Password.

c) Access to the Internet from the Municipal internal network shall only be through secure established links employing secure firewall technology and only with recommended browsers.

d) For all other Internet connections where connectivity to the firewall is not yet available, the user is required to use a stand alone workstation (i.e.not connected to the Municipal Network to gain access via an Internet provider approved or supplied by the Department: Information Communication Technology.

e) Connection to the Internet with a modem while a workstation is still connected to the municipal network is not secure for the network and is therefore prohibited. Any computer or independent dial-up to any external computer or network must therefore be physically isolated from the Municipality's internal networks. Use of a modem while connected to the Municipal network is an offence and the Municipality may take appropriate corrective action against any person who does not observe this rule. This rule also applies to Secure Dial-up connections provided by the Municipality.

f) Downloading of any software from the Internet is prohibited. Should a user require this facility, he/she must contact the Manager: ICT

g) Publishing Municipal information directly on the Internet is prohibited. If a user requires information to be published on the Internet, he/she must do this via the Manager: Communications.

h) Internet Access User IDs may not be shared with other persons and a user may not use an Internet Access account assigned to another individual to gain access to the Internet.

i) Users are not permitted to establish, maintain, or promote personal home pages using the Municipality's assets, resources or name.

2.5 Legal, Marketing and regulatory requirements.

a) Compliance with legal requirements is mandatory. Such requirements include, but are not restricted to intellectual property rights, trademark laws and copyright laws. No third-party materials or photographs must be used or forwarded using any Municipal resource without obtaining the prior written permission of the owner.

b) All Municipal-related information that is to be sent out over the Internet is to be reviewed for compliance with ethical, industry, and national regulatory requirements.

c) The Municipality's claims of copyright and trademark in intellectual property dissemination on the Internet must be identified clearly.

2.6. Restrictions on disclosing confidential information of the Municipality

Regardless of the availability of encryption methods or other security measures, it must be assumed that the Internet or other online services are not adequately equipped to protect information that is considered highly sensitive, confidential or personal. Before disseminating information that is considered to be confidential and/or proprietary business or technical information of the Municipality, users should carefully consider the nature of the information being disclosed and whether another method of communication is more appropriate. If a user is uncertain whether information is confidential, he or she shall request a ruling from the Municipality's Information Officer and must abide by such ruling.

3. ICT INFRASTRUCTURE BUSINESS REQUIREMENTS

In order to stabilse the ICT network and to ensure a standardised maintainable ICT infrastructure at the most economic cost, the following shall apply:

3.1 Procurement of ICT infrastructure

a) All purchases if ICT and ICT related equipment, software, systems or training must be dealt with by the Department: Information Communication Technology

b) Digital and video cameras, data projectors, USB sticks of all kind,scanners, printers and photo copy machines are, for purposes of paragraph 3.1.1 above, regarded as ICT equipment.

3.2 Desk Top Software

a) Workstations and notebooks shall be provided with a basic standard workstation/notebook software setup consisting of word processor, spreadsheet and presentation software as a general rule.

b) Requests for additional software over and above those mentioned in paragraph a) above must be motivated through the user's Manager as a business requirement and submitted to the ICT Steering Committee for consideration.

3.3 Workstations and Notebooks

a) The make of workstations and notebooks to be procured must, as far as possible, be standardised so as to obtain the best price/performance ratio, the lowest cost of maintenance and the best possible supplier support.

b) The standardisation referred to in paragraph a) must be considered and determined by the ICT Steering Committee.

c) Workstations and/or notebooks replaced with new ones and which are still economically usable must be redeployed by the Department: ICT unless the relevant Director has motivated the redeployment of the replaced workstations or notebooks within his/her directorate for business reasons.

3.4 Printers

a) Personal printers shall, in order to cater for confidentiality issues and special requirements, be issued to the Executive Mayor and his Personal Assistant, the Municipal Manager and his Personal Assistant and Directors and their Secretaries.

b) All other users are restricted to the use of network printers in close proximity to their local group.

c) Deviations from the provisions of paragraph b) may only be considered by the ICT Steering Committee upon a written request and motivation by an affected user and fully supported by his/her director.

4. NON-COMPLIANCE

a) All users are responsible for complying with this policy, as well as any guidelines and standards developed in support of this policy. Failure to comply with the conditions of this policy shall lead to appropriate corrective action being taken against the user concerned.

b) Violations of procedures, standards or practices in support of this policy shall be brought to the attention of management for appropriate action.

5. APPLICATION OF THIS POLICY

a) The provisions of this policy shall apply to the whole of the Municipality, its Municipal associates and employees and to any vendor and/or contractor or consultant utilising any Municipal provided computer, software, network service or any other Municipal information system or service.

b) This policy shall apply to the use of all Municipal computers, including laptops, either on or off the Municipality's premises, during or outside of normal working hours.

Policy Section	Information Communication Technology
Current Update	29 August 2012
Previous Review	28 March 2012
Approval by Council	25 August 2010