

## COUNCIL POLICY

SUBJECT : ELECTRONIC COMMUNICATIONS POLICY

REFERENCE : 6.2.2.B

RESOLUTION NR : 23.4/08/2005      DATE : 29 August 2005

POLICY OBJECTIVE : The **purpose** of this Policy is to:

- \* Inform and educate users on the access to and use of the municipality's communication facilities and equipment;
- \* Create rules for the access to and use of the municipality's communication facilities and equipment;
- \* Provide for the interception of communications;
- \* Provide for disciplinary action against users who fail to comply with this Policy; and
- \* Ensure and maintain the value and integrity of the municipality's equipment and network(s).

### POLICY PHILOSOPHY AND PRINCIPLES

Council aims to facilitate and ensure good business practices in electronic communications.

### GUIDELINES

#### 1. RATIONALE

//Khara Hais Municipality ("*//Khara Hais*") has a legal right and duty to:

- \* Secure and maintain its computer network, equipment and communication facilities;
- \* Comply with the provisions of laws and regulations that govern the access, use and interception of communications;
- \* Protect the privacy of its clients;
- \* Identify and address the potential risks associated with the use of technology and Communication Facilities in the workplace;
- \* Promote employee productivity;
- \* Ensure the confidentiality of //Khara Hais's trade secrets, client information, employee information and confidential information generally;

- \* Investigate and prosecute illegal or unauthorized use of its communication facilities and/or equipment; and
- \* Respect and protect every employee's right to privacy, free speech and the right to receive and impart with information as detailed, amongst others, in the Constitution of South African, 1996.

To successfully discharge the above-mentioned obligations //Khara Hais needs to:

- \* Regulate employee use of equipment and communication facilities;
- \* Monitor and intercept employee communications; and
- \* Secure and maintain the equipment and communication facilities, as detailed in, amongst others, this Policy.

## 2. DEFINITIONS

*"Communication facilities"* include Internet access, e-mail access and use of any Equipment for purposes of:

1. accessing, creating, copying, distributing, sharing and deleting records; or
2. initiating, creating, receiving or storing communications.

*"Communications"* include:

1. oral and verbal utterances of a user in or during a meeting where the business of //Khara Hais or related matters are discussed;
2. the transfer of any information whether speech, data, text, signals, radio frequency spectrum, images in any format through communication facilities; and
3. access to or use of the services available on the Internet, including e-mail, instant messaging, websites, file transfer, video conferencing, voice over IP, chat rooms and bulletin boards by users through the equipment.

*"Discriminatory"* means offensive, untrue or provocative material based on race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth;

*"Equipment"* means computers, desktops, servers, routers, laptops, telephones, cell phones, electronic handheld devices, facsimile machines, pagers, software, hardware and/or similar equipment owned by, licensed to or rented by //Khara Hais;

**"Illegal Content"** means material that is pornographic, discriminatory, oppressive, racist, hate speech, sexist, defamatory against any user or third party, offensive to any user or group, a violation of a user's or a third party's privacy, identity or personality, copyright infringement, malicious codes such as viruses and trojan horses, and content containing any personal information of third parties without their express consent and includes hyperlinks or other directions to such content;

**"Intercept"** means filter, scan, block, redirect, access, disrupt, copy, print, disclose, retain, use, collect, delete and/or record, in any format and in any manner;

**"Internet"** shall in all cases include //Khara Hais's intranet, mobile networks or wireless access areas;

**"Monitor"** includes to listen to or record communications by means of a monitoring device;

**"Monitoring Device"** means any electronic, mechanical or other instrument device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication;

**"Personal Information"** means personal information as defined in the Promotion of Access to Information Act;

**"Policy"** means this Electronic Communications Policy;

**"Pornographic"** means all the content and actions, simulated or real, graphic or written detailed in Schedules 1, 2, 6, 7 and 11 of the Films and Publications Act 65 of 1996;

**"Record"** means any content, document, record, file, data, information, picture, download, graphic, depiction, representation or software that is created, used, accessed, disclosed, copied, stored, received or delivered by a user, regardless of the format thereof; and

**"User(s)"** mean all persons who have access to or use of //Khara Hais Equipment, communication facilities or communications.

### 3. ACCEPTABLE USE AND GENERAL GUIDELINES

This paragraph details general guidelines for the access and use of //Khara Hais's equipment and communication facilities:

- 3.1 Users shall use e-mail and Internet access primarily for //Khara Hais business purposes. Without prejudice to //Khara Hais's right to block certain e-mails and internet access, private and personal use shall be tolerated, subject to the rules detailed in this policy as mentioned in paragraph 4.
- 3.2 When forwarding or replying to e-mail messages, the contents of the original message should not be altered. If the contents need to be changed, then all changes must be clearly marked as such;
- 3.3 //Khara Hais has the right to limit the size of incoming and outgoing e-mail messages and attachments, downloads and other files and may block and delete e-mail messages, downloads, attachments or other files that are larger than the set maximum size. It is the responsibility of users to limit the size of attachments and other files to prevent overloading of equipment;
- 3.4 E-mail messages should be kept brief and formulated appropriately;
- 3.5 Virus warnings or pop-ups that result from incoming e-mail or file downloads must be reported to the IT department immediately;
- 3.6 All outgoing e-mails must have the municipality's legal notice at the top of the message. This e-mail legal notice may not be removed or tampered with by users;
- 3.7 Users must check e-mail recipients prior to sending, forwarding or replying to messages. When distribution lists are used the sender should consider whether or not each group member really needs, or really should, receive the e-mail;
- 3.8 The subject field of an e-mail message should relate directly to the contents or purpose of the message;
- 3.9 Users must log-off from systems or use screen savers with passwords in times of absence from a computer terminal to avoid improper and/or illegal use;
- 3.10 Notebook and/or offline users should load and update the "*address book*", if any, regularly; and
- 3.11 If users are out of the office for more than one day, they should activate the "*out of office*" function. This informs the sender of an e-mail of the user's absence. The "*out of office*" message should include both the period of absence and an

alternative contact person.

3.12 Only the IT Official shall setup passwords allowing access to any computer or terminal. Such passwords must be duly documented and kept in a safe place.

#### 4. NON – ACCEPTABLE AND PUNISHABLE USE

The following communications, actions or forms of content are prohibited and punishable:

- 4.1 Sharing log on usernames with or disclosing passwords to any third person(s);
- 4.2 Modify ing an e-mail message and forwarding or reply ing therewith without noting the changes (i.e. deletions, removal of recipients, modification of content, etc.);
- 4.3 Fabricating a message and/or sender of a message;
- 4.4 Intentionally bypassing the security mechanisms of the Equipment or any third party security system or website;
- 4.5 Modify ing the internal mail transport mechanism to forge a routing path that a message takes through the Internet;
- 4.6 Illegal Content;
- 4.7 Participating in e-mail "*chain letters*" or similar activities;
- 4.8 Downloading, receiving, using and/or installing software applications not approved by the IT-department;
- 4.9 Knowingly burden //Khara Hais's equipment or communication facilities with data unrelated to //Khara Hais's official business (e.g. forwarding, downloading or accessing large video clips or graphics to or from a distribution list or file-sharing server);
- 4.10 Using automatic forwarding of e-mails ("*auto rules*") to any person without such person's consent;
- 4.11 The creation, sending or forwarding of unsolicited mail (spam);
- 4.12 The creation, sending or forwarding of marketing information or advertising material unrelated to //Khara Hais' official business;

- 4.13 Sending or forwarding messages and attachments that are infected with malicious codes such as viruses;
- 4.14 Using discs that may be infected with malicious code;
- 4.15 Using any encryption, authentication and/or digital signatures not authorized by the IT Department in writing;
- 4.16 Playing, downloading, reproducing, sharing, retaining and/or creating records that contain music, images, sound or video if such record is prohibited by copyright or law or not reasonably required for the user's official //Khara Hais services;
- 4.17 Accessing and using internet relay chat if such actions burden //Khara Hais' equipment or communication facilities;
- 4.18 Any actions that knowingly prevent other users from using and accessing equipment or communication facilities;
- 4.19 Taking any of the steps or actions criminalized and detailed in Chapter XIII of the Electronic Communications and Transactions Act, 2002 (Act 25 of 2002), including but not limited to hacking or developing, downloading and using any technology that may circumvent IT-security measures;
- 4.20 Any destructive and disruptive practices on, through or with equipment or communication facilities;
- 4.21 Indiscriminate storage and/or forwarding of e-mail, files, websites and attachments for which permission has not been obtained from the originator or copyright holder;
- 4.22 Any purposes that could reasonably be expected to cause directly or indirectly excessive strain on any computing facilities, or unwarranted or unsolicited interference with others;
- 4.23 Sending, replying to or forwarding e-mail messages or other electronic communications which hide the identity of the sender or represents the sender as someone else; and
- 4.24 Using or accessing //Khara Hais's equipment or communication facilities to commit fraud or any other criminal offence(s).

## PROCEDURES

### 1. SCOPE OF APPLICATION

This Policy applies to all users as well as third parties that have temporary access to and/or use of //Khara Hais's communication facilities or equipment.

### 2. RESPONSIBLE PERSONS AND RIGHT TO MONITOR

#### 2.1 RESPONSIBLE PERSONS

2.1.1 Users are personally responsible to abide by the rules created in this Policy.

2.1.2 The Information Technology department is responsible for:

1. The technical issues related to the access to and use of //Khara Hais's communication facilities and equipment;
2. Assisting //Khara Hais' management in intercepting communications and investigating breaches of the provisions of this Policy;
3. Causing all outgoing e-mail messages to contain //Khara Hais' official e-mail legal notice; and
4. Scan, filter and block all electronic communications for damaging code such as viruses.

2.1.3 The Administration is responsible for the implementation, communication, maintenance and management of this Policy.

2.1.4 The Subdirector Human Resources is responsible for bringing this Policy to the attention and access of all users and ensuring that every user agrees in writing to //Khara Hais's right to intercept any communications and to take disciplinary actions in terms of this Policy.

2.1.5 All officials are responsible for updating information on the systems relating to the authority of the position held in employment.

#### 2.2 RIGHT TO MONITOR

2.2.1 //Khara Hais reserves the right to intercept any communication and/or record if such

interception is reasonably required and justified for one or more of the following purposes:

1. Compliance with //Khara Hais's obligations detailed in clause 3.1 above;
2. Investigating, preventing or detecting unauthorized access or use;
3. Investigating, preventing or detecting breach of the provisions of this Policy;
4. Maintenance of the security of any equipment or communication facilities;
5. Disaster recovery or similar emergency measures;
6. Prevention of loss or destruction of //Khara Hais assets or data; and
7. Investigating or detecting illegal activities.

2.2.2 //Khara Hais's right to intercept any communication shall:

1. Only commence with the prior written authority of the Municipal Manager; and
2. Be implemented with due regard to the privacy and constitutional freedom of users.

2.2.3 Any person who actually intercepts communications or has access to intercepted communications shall sign a non-disclosure agreement prior to such interception and undertake not to disclose the interception process, the identity of subject and/or any related information, unless authorized to do so by due legal process or for the purposes of disciplinary or legal action.

2.2.4 //Khara Hais shall not share or disclose the following information to third parties:

1. Private, personal and confidential information collected through the interception of communications; or
2. The identity of users whose communications are or were the subject of interception, unless such disclosure is authorized by due legal process or for the purpose of disciplinary or legal action.

3. DELETION OF E-MAIL

Users shall manage and store e-mails as detailed in //Khara Hais's Records Management Policy.

4. AUTHORISED E-MAIL AND INTERNET USERS

The attached document is a detailed list of all officials who have access to e-mail and internet.

Business e-mails are sent to the post and not to an individual. For sound business practice and continuity, addresses will not be changed.

1. Access to internet and e-mail proceed via Council's network.
2. Only one telephone connection is connected to the network that ensures access outside.
3. Access to this facility serve as a communication method through which business activities are administered, better friendly and speedily.
4. An access code and password identify a user to the Internet. The access code will have direct relation with the post holder's name.
5. For security and other control measures, access to the Internet is assigned to a person for the equivalent employed period.
6. Where a user has been allocated with an access code and password and such user provide other users with his/her access code and password, the authorised user will be held liable for any misuse.

5. DUTY TO DISCLOSE & REPORT

Users have the duty to disclose all true or suspected attempts that may reasonably breach any provision of this Policy to the Municipal Manager.

6. CONSEQUENCES OF MIS-USE

Failure and/or refusal to abide by the rules detailed in this Policy shall be deemed as misconduct and //Khara Hais may initiate the appropriate investigation and disciplinary action against users. Such steps may include dismissal or expulsion, as the case may be.

7. USE OF INTERNET

1. The Internet is a medium through which information is provided to the world in an electronic format. The Council wants to share in the availability if this information.
2. Access to the internet is restricted to the following posts on the Council's service record:
  - 2.1 **Council**  
Mayor  
Speaker
  - 2.2 **Office of the Municipal Manager**

Municipal Manager  
Personal Assistant of the Municipal Manager  
Chief : Internal Audit  
Tourism Marketing Official  
Public Relations Officer  
Economic Developer

2.3 **Directorate Development Services**

Director Development Services  
Personal Assistant of the Director Development Services  
Chief Human Resources  
Senior Personnel Officer  
Organisational and Work-study Official  
Administrative Official GrII  
Chief Environmental Services  
Chief Traffic Services  
Chief Fire Brigade  
Chief Security Services

2.4 **Directorate Corporate Services**

Director Corporate Services  
Personal Assistant of the Director Corporate Services  
Chief Administration  
Senior Administrative Official  
Senior Librarian  
Transport and Control Officer  
Chief Finances  
Deputy Chief Finances  
Chief Accountant  
Information Technology Official  
Computer Technician

2.5 **Directorate Technical Services**

Director Technical Services  
Chief Civil Services  
Chief Electrical Services  
Chief Town Planning and Building Control

3. Users identify themselves with access code and a password. The access code will

be directly linked to the title of the user's post.

4. For security and other control measures internet access are made accessible to a user while such user occupies an approved post.
5. Where more than one person uses the same access code and password security and control measures are thrown overboard, because it cannot be determine who uses the facility at a specific time. Therefore the person to which an access code is allocated is responsible for any misuse.

8. USE OF ELECTRONIC MAIL (E-MAIL)

1. E-mail is a electronic postal address to which post is send in electronic format for quicker disposing thereof.
2. The Council's electronic postal addresses is composed as follow:

code@kharahais.gov.za

3. Only the following posts on the Council's record of service will have access to electronic postal addresses through the code next to it:

3.1 **Council**

Mayor	mayor
Speaker	speaker
Clerk Grd II/ Secretary	mayorsec

3.2 **Office of the Municipal Manager**

Municipal Manager	manager
Secretary	managersec
Chief Internal Audit	audit
Tourism Marketing Official	tourism
Public Relations Officer	pro
Economic Developer	dev

3.3 **Directorate Corporate Services**

Director Corporate Services	corp
Personal Assistant to the Director Corporate Services	corpsec
Chief Administration	admin
Senior Administrative Official	senao
Administrative Official Committees	adminoc
Administrative Official Gr II	adminoa
Administrative Official GrII (Mayor)	adminom
Senior Typist	adminsec

Senior Librarian	library
Library Assistant Paballelo	pablib
Library Assistant Forum	forum
Transport and Control Official	transp
Superintendent Workshop	supws
Manager Holiday Resorts	resort
Tourism Official	resorto
Chief Finance	finance1
Deputy Chief Finance	finance3
Assistant Chief Finance	finance4
Chief Accountant	finance2
Senior Accountant Housing	rates1
Assistant Accountant	rates2
Senior Clerk Services	services
Senior Accountant Income	income
Senior Accountant Expenditure	expences
Chief Clerk Salaries	salaries
Senior Accountant Stores	stores
Storekeeper/Purchaser	buyer
Information Technology Official	it

### 3.4 Directorate Development Services

Director Development Services	dev
Personal Asst to the Director Development Services	devsec
Chief Traffic Services	traffic
Chief Fire Services	fire
Chief Security Services	security
Chief Environmental Services	henvhealth
Chief Human Resources	personel
Administrative Official GrII	persadmin
Client Services Official	client
Personnel Officer	personelo
Organisational and Workstudy Official	two
Clerk Grd I Typist (Environmental Health)	envhealth
Environmetal Health Officials x 4	envhealth1 ...4

### 3.5 Directorate Technical Services

Director Technical Services	tech
Personal Assistent to the Director Technical Services	techsec
Chief Civil Engineering Services	civil
Chief Electrical Services	elec
Control Technician (Civil Services)	techserv
Control Technician (Water Purification)	techwater
Chief Town Planning and Building Control	planning

ROLES

Municipal Manager

Directors

Heads of Sub Directorates

All Municipal Officials

Media committee

RELATED POLICIES

Access to Information Act, Act 2, 2000.

Administrative Justice Act, Act 3, 2000.

Films and Publications Act, Act 65, 1996; and

Electronic Communications and Transactions Act, Act 25, 2002.

Corporate Communication policy .

//Khara Hais Filing system.

User access to internet and e-mail policy .

Code of good practice.