MUNISIPALITEIT DAWID KRUIPER MUNICIPALITY

POLICY 036/2017 RAADSBELEID

SUBJECT/ONDERWERP: **ELECTRONIC COMMUNICATION POLICY**

REFERENCE/VERWYSING: **6.1.3**

RESOLUTION NR/BESLUIT NO: **14.3/05/2017 (SCM)** DATE/DATUM: **30 MAY 2017**

1 POLICY OBJECTIVE

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

- Inform and educate Users on the access to and use of Dawid Kruiper's Communication Facilities and Equipment;
- Create rules for the access to and use of Dawid Kruiper'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).

2 POLICY PHILOSOPHY AND PRINCIPLES

Regulate the use of communication equipment and facilities by ensuring good business practice.

3 GUIDELINES

3.1 RATIONALE

Dawid Kruiper Municipality ("*Dawid Kruiper*") 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 Dawid Kruiper's trade secrets, client information, employee information and confidential information generally;

- Investigate and prosecute illegal or unauthorised use of its Communication Facilities and/or Equipment;
- 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 South African Constitution of 1996.

To successfully discharge the abovementioned obligations Dawid Kruiper 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 Dawid Kruiper Electronic Communications Policy.

3.2 DEFINITIONS

"***Communication Facilities***"include Internet access, email access and use of any Equipment for purposes of:

a) accessing, creating, copying, distributing, sharing and deleting Records; or

b) initiating, creating, receiving or storing Communications.

"***Communications***" include:

a) oral and verbal utterances of a User in or during a meeting where the business of Dawid Kruiper or related matters are discussed;

b) the transfer of any information whether speech, data, text, signals, radio frequency spectrum, images in any format through Communication Facilities; and

c) access to or use of the services available on the Internet, including email, 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 Dawid Kruiper;

"***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 Dawid Kruiper'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 Dawid Kruiper's Equipment, Communication Facilities or Communications.

3.3 ACCEPTABLE USE AND GENERAL GUIDELINES

This paragraph details general guidelines for the access and use of Dawid Kruiper's Equipment and Communication Facilities:

3.3.1 Users shall use email and Internet access primarily for Dawid Kruiper business purposes. Without prejudice to Dawid Kruiper's right to block certain emails and internet access, private and personal use, in moderation, shall be tolerated, subject to the rules detailed in this policy. Common sense and good judgment should guide personal and private usage;

3.3.2 When forwarding or replying to email 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;

3.3.3 Dawid Kruiper has the right to limit the size of incoming and outgoing email messages and attachments, downloads and other files and may block and delete email 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;

3.3.4 Email messages should be kept brief and formulated appropriately;

3.3.5 Virus warnings or pop-ups that result from incoming email or file downloads must be reported to the IT department immediately;

3.3.6 All outgoing emails must have the municipality's legal notice at the top of the message. This email legal notice may not be removed or tampered with by Users;

3.3.7 Users must check email 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 email;

3.3.8 The subject field of an email message should relate directly to the contents or purpose of the message;

3.3.9 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;

3.3.10 Notebook and/or offline Users should load and update the "address book", if any, regularly; and

3.3.11 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 email of the User's absence. The "Out of Office" message should include both the period of absence and an alternative contact person.

3.3.12 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.

3.4 NON – ACCEPTABLE AND PUNISHABLE USE

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

3.4.1 Sharing logon usernames with or disclosing passwords to any third person(s);

3.4.2 Modifying an email message and forwarding or replying therewith without noting the changes (i.e. deletions, removal of recipients, modification of content, etc.);

3.4.3 Fabricating a message and/or sender of a message;

3.4.4 Intentionally bypassing the security mechanisms of the Equipment or any third party security system or website;

3.4.5 Modifying the internal mail transport mechanism to forge a routing path that a message takes through the Internet;

3.4.6 Illegal Content;

3.4.7 Participating in email "chain letters" or similar activities;

3.4.8 Downloading, receiving, using and/or installing software applications not approved by the IT department;

3.4.9 Knowingly burden Dawid Kruiper's Equipment or Communication Facilities with data unrelated to Dawid Kruiper's official business (e.g. forwarding, downloading or accessing large video clips or graphics to or from a distribution list or file-sharing server);

3.4.10 Using automatic forwarding of emails ("Auto Rules") to any person without such person's consent;

3.4.11 The creation, sending or forwarding of unsolicited mail (spam);

3.4.12 The creation, sending or forwarding of marketing information or advertising material unrelated to Dawid Kruiper's official business;

3.4.13 Sending or forwarding messages and attachments that are infected with malicious codes such as viruses;

3.4.14 Using discs that may be infected with malicious code;

3.4.15 Using any encryption, authentication and/or digital signatures not authorized by the IT Department in writing;

3.4.16 Playing, downloading, reproducing, sharing, retaining and/or creating Records that contain music, images, sound or video if such Record is not reasonably required for the User's official Dawid Kruiper services;

3.4.17 Accessing and using internet relay chat if such actions burden Dawid Kruiper's Equipment or Communication Facilities;

3.4.18 Any actions that knowingly prevent other Users from using and accessing Equipment or Communication Facilities;

3.4.19 Taking any of the steps or actions criminalised and detailed in Chapter XIII of the Electronic Communications and Transactions Act 25 of 2002, including but not limited to hacking or developing, downloading and using any technology that may circumvent IT security measures;

3.4.20 Any destructive and disruptive practices on, through or with Equipment or Communication Facilities;

3.4.21 Indiscriminate storage and/or forwarding of email, files, websites and attachments for which permission has not been obtained from the originator or copyright holder;

3.4.22 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;

3.4.23 Sending, replying to or forwarding email messages or other electronic communications which hide the identity of the sender or represents the sender as someone else; and

3.4.24 Using or accessing Dawid Kruiper's Equipment or Communication Facilities to commit fraud or any other criminal offence(s).

4 PROCEDURES

4.1 SCOPE OF APPLICATION

This Policy applies to all Users as well as third parties that have temporary access to and/or use of Dawid Kruiper's Communication Facilities or Equipment.

4.2 OWNERSHIP, RESPONSIBLE PERSONS AND RIGHT TO MONITOR

4.2.1 RESPONSIBLE PERSONS AND DUTIES

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

4.2.2.1 The Dawid Kruiper's IT department is responsible for:

- the technical issues related to the access to and use of Dawid Kruiper's Communication Facilities and Equipment;
- assisting Dawid Kruiper's management in Intercepting Communications and investigating breach of the provisions of this Policy;
- causing all outgoing email messages to contain Dawid Kruiper's official email legal notice; and
- scan, filter and block all electronic Communications for damaging code such as viruses.

4.2.2.2 Dawid Kruiper's Sub Directorate Administration is responsible for the implementation, communication, maintenance and management of this Policy.

4.2.2.3 Dawid Kruiper's Sub Directorate Human Resources is responsible for bringing this Policy to the reasonable attention and access of all Users and ensuring that every User agrees in writing to Dawid Kruiper's right to intercept any Communications and to take disciplinary actions in terms of this Policy.

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

4.2.2 RIGHT TO MONITOR

4.2.2.1 Dawid Kruiper 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:

4.2.2.1.1 Compliance with Dawid Kruiper's obligations detailed in clause 3 above;
4.2.2.1.2 Investigating, preventing or detecting unauthorized access or use;
4.2.2.1.3 Investigating, preventing or detecting breach of the provisions of this Policy;
4.2.2.1.4 Maintenance of the security of any Equipment or Communication Facilities;
4.2.2.1.5 Disaster recovery or similar emergency measures;
4.2.2.1.6 Prevention of loss or destruction of Dawid Kruiper assets or data; and
4.2.2.1.7 Investigating or detecting illegal activities.

4.2.2.2 Dawid Kruiper's right to Intercept any Communication shall:

4.2.2.2.1 Only commence with the prior written authority of the Municipal Manager; and
4.2.2.2.2 Be implemented with due regard to the privacy and constitutional freedoms of Users.

4.2.2.3 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.

4.2.2.4 Dawid Kruiper shall not share or disclose the following information to third parties:

4.2.2.4.1 Private, personal and confidential information collected through the interception of Communications; or

4.2.3.4.2 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 purposed of disciplinary or legal action.

4.3 DELETION OF EMAIL

Users shall manage and store emails as detailed in Dawid Kruiper's Records Management Policy.

4.4 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.

4.5 CONSEQUENCES OF MIS-USE

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

5 ROLES

Municipal Manager
Directors
Heads of Sub Directorates
All Municipal Officials
Media committee

6 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
Dawid Kruiper Filing system
User access to internet and email policy

REPEAL

That all previous resolutions/policies regarding this matter be repealed.