



elrc

EDUCATION LABOUR
RELATIONS COUNCIL

**IT Internet And Email
Policy & Procedures
Manual**






 <p>elrc EDUCATION LABOUR RELATIONS COUNCIL</p>	<p>EDUCATION LABOUR RELATIONS COUNCIL</p>	<p>Doc No. IT/PC/002</p>	
		<p>Date: APRIL 2016</p>	<p>Rev 0</p>
		<p>Page: 2 of 8</p>	
<p>Title: IT INTERNET AND EMAIL POLICY & PROCEDURE MANUAL</p>		<p>Document type: POLICY</p>	
<p>This document has been seen and accepted by the following: EXECUTIVE COMMITTEE OF THE COUNCIL</p>		<p>COMPILED/ REVIEWED BY:</p>  <p>DAKALO NEMAVHOINI IT MANAGER</p>	
<p>RECOMMENDED BY:</p>  <p>OCTAVIA MAKOFANE SENIOR MANAGER: CS</p>	<p>APPROVED BY:</p>  <p>NOLUSINDISO FOCA GENERAL SECRETARY</p>	<p>AUTHORISED BY:</p>  <p>LUVUYO BONO CHAIRPERSON OF THE COUNCIL</p>	
<p>DATE OF LAST REVIEW: APRIL 2016</p>			
<p>DATE OF NEXT REVIEW: APRIL 2018 NOTE: - This document may be changed before the stipulated period as and when a need arises as guided by the Documentation Policy.</p>			

TABLE OF CONTENTS

	Page
1. ACRONYMS AND DEFINITIONS	4
2. PURPOSE	4
3. LEGAL FRAMEWORK	4
4. OBJECTIVES OF THE POLICY	4
5. SCOPE OF APPLICATION	5
6. POLICY STATEMENTS	5
7. POLICY REVIEW	8

1. ACRONYMS AND DEFINITIONS

IT	Information Technology
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
INFORMATION ASSET	Refers to electronic data, information, business application systems, operating systems, computer equipment and other IT infrastructure.
SHAREPOINT	A web application platform developed by Microsoft.
MB	Megabyte, a measure of amount of information used, for example, to quantify computer memory or storage capacity.

2. PURPOSE

- 2.1 The purpose of this policy is to prevent tarnishing the public image of ELRC. When an email goes out from ELRC, the general public tends to view that message as official communication from the ELRC.

3. LEGAL FRAMEWORK

- 3.1 SITA Act, of 1998.
- 3.2 Public Service Act, No 103 of 1994.

4. OBJECTIVES OF THE POLICY

The purpose of this policy is to ensure that:

- 4.1 ELRC employees are informed about the applicability of the policy with regard to email and internet usage.
- 4.2 Disruptions to ELRC email and other service activities are minimised.

5. SCOPE OF APPLICATION

- 5.1 This policy is applicable to all users who make use of the ELRC's information resources. All users and staff to whom such resources are available are aware of the policy and act in accordance with it. The policy also applies to all temporary staff, service providers, or consultants.

6. POLICY STATEMENTS

6.1 Background

Email is an efficient and timely communications tool that is provided by the ELRC to assist in supporting the organisation's functions. Appropriate use of the ELRC email system can enhance productivity and communication, but inappropriate use can conflict with ELRC policies and compromise availability of the system for all. This policy defines requirements and prohibitions for appropriate use of the ELRC email system that uses the ELRC computer network.

6.2 Principles (Email)

6.2.1 Examples of limited permitted personal use of electronic mail system include a message to a few employees, arranging lunch or retirement party for a co-worker, etc.

6.2.2 Example of personal use that is not permitted include chain letters, advertising items for sale, pornography, etc.

6.3 Prohibited use

6.3.1 The ELRC email system shall not to be used for the creation or distribution of any disruptive or offensive messages, comments about race, gender, hair, colour, disabilities, age, sexual orientation, pornography, religious beliefs, or national origin. Employees who receive any emails with this content from any ELRC employee should report the matter to their manager immediately.

6.3.2 ELRC employees shall not be allowed to send email attachments exceeding 10MB, should there a requirement to send an email exceeding 10MB to external parties, employees must make arrangements with Helpdesk. If an email is to be sent to more than five people on the ELRC network and is 10MB or more, it must go to SharePoint. If an email needs to be sent outside the department, the email will be released only after hours to reserve bandwidth to prevent high network utilisation.

6.4 Personal Use

6.4.1 Using a reasonable amount of ELRC resources for personal emails is not allowed. Sending chain letters or joke emails from an ELRC email account is prohibited. Virus or other malware warnings and mass mailings from the

ELRC shall be approved by the IT Manager before sending. These restrictions also apply to the forwarding of Mail received by ELRC employees.

6.5 Disclaimer

6.5.1 All email communication intended for external recipients shall include the ELRC disclaimer.

6.5.2 **ELRC Disclaimer:** This message and any attachments are confidential and intended solely for the addressees. If you receive this message in error, please delete it and immediately notify the sender. If the reader of this message is not the intended recipient, you are hereby notified that any unauthorised use, copying or dissemination is prohibited. E-mails are susceptible to alteration. Neither the Education Labour Relations Council (ELRC), nor any of THE Parties to Council shall be liable for the message if altered, changed or falsified.

6.6 Email Signature

6.6.1 A standard email signature must be used; personal signatures, photos and any other images are prohibited. Below is an example of the approved ELRC email signature:



Dakalo Nemavhoini
ICT Manager: Corporate Services
☐ +27 12 663 7446 |
☐ +27 12 663 9604
☐ +27 76 184 5544

☐ Dakalon@elrc.org.za |
www.elrc.org.za
ELRC Building, 261 West Avenue,
Centurion, 0046

6.7 Non Guarantee

6.7.1 The ELRC does not guarantee that email communication will be successfully delivered. When sending important email messages; ELRC employees must verify the successful delivery of the message i.e. requesting conformation.

6.8. Monitoring

6.8.1 ELRC employees shall have no expectation of privacy in anything they store, send or receive on the Council's system. The ELRC may monitor messages without prior notice. The ELRC is not obliged to monitor email messages.

6.9 Principles (Internet)

6.9.1 Access to the internet shall be granted appropriately according to the role or function for service required according to the user's role as defined by the HR Department. Internet Services (FTP, HTTP(s)) shall only be granted with prior with written authorisation from the Senior Manager/Line Manager.

6.10 Prohibited Use

6.10.1 ELRC internet shall not be used for the following:

6.10.1.1 Accessing sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal material;

6.10.1.2 Conducting fraudulent activities;

6.10.1.3 Stealing, using, or disclosing someone else's password without authorisation;

6.10.1.4 Downloading, copying or pirating software and electronic files that are copyrighted or without authorisation;

6.10.1.5 Hacking into unauthorised websites;

6.10.1.6 Introducing malicious software onto the ELRC network and/or jeopardizing the security of the ELRC's IT systems;

6.10.1.7 Audio streaming and watching videos online (YouTube).

6.11 Personal Use

6.11.1 Any personal use of the internet must be incidental to the assigned job duties. Secondly, personal use must not interfere with the employee performance and/or be disruptive in the workplace.

6.12 SharePoint

6.12.1 All ELRC employees shall use SharePoint as a platform for document management in line with the Council's file plan (i.e. creation, modification and storing of documents), collaboration and online forums for discussions.

6.13 Monitoring

6.13.1 The IT Department will log and monitor activities, time spent and destinations on the internet.

6.13.2 The ELRC reserves the right to divulge and make public any such information that is logged and captured against the respective user.

6.14 Roles and Responsibilities

Issue	Personal Responsible	Alternate
Has overall responsibility for adherence to policy	ELRC Senior Manager: CS	ELRC IT Manager
Has the responsibility for implementation and adherence to the policy	IT Manager	
Adherence to the policy	All ELRC employees	

6.15. Security Violation and Disciplinary Measures

- 6.15.1 Any attempts to bypass security controls or to obtain unauthorised access or to make unauthorised use of a user account belonging to someone else shall be considered a security violation.
- 6.15.2 The use of ELRC information assets for purposes other than for authorised business purposes shall be considered a security violation.
- 6.15.3 The use of ELRC's information assets for any unauthorised or illegal activity shall be considered a security violation.
- 6.15.4 Any act (or failure to act) that constitutes or causes a security incident or creates security exposure shall be considered a security violation.
- 6.15.5 Any act (or failure to act) that results in sensitive or critical business information being disclosed to an unauthorised person, shall be considered a security violation.
- 6.15.6 Any act (or failure to act) that results in sensitive or critical business information being modified or destroyed such that the ELRC or any of its branches/ sub branches is adversely impacted, shall be considered a security violation.
- 6.15.7 Any breach of this policy or any of its related documents shall be considered a security violation.
- 6.15.8 Any person charged with a security violation shall face disciplinary action.
- 6.15.9 All information abuses and security breaches should be reported to the IT Manager.

7. POLICY REVIEW

The policy shall be reviewed annually or as and when the need arise with permission from the General Secretary.