Lejweleputswa District Municipality

Information Communications Technology

TECHNOLOGY USAGE POLICY

1. Table of Contents

2. Definitions

- **Attachments:** Files created in other applications (such as Ms-Word, MS-Excel) or pictures.

- **E-Mail:** An electronically transmitted message, along with attachments and any information appended by the e-mail system.

- **E-Mail System:** Computer hardware and software system that allows personal computer users to send, receive and store messages, documents and files with other individuals or groups of people over an internal network or the Internet.

- **Encryption:** A means of coding messages so they appear to be random characters. Encryption has two benefits. First, it prevents disclosure of sensitive information to unauthorized third-parties. Second, encryption allows for "authentication" of the information sent.

- **Freeware:** Programming that is offered at no cost, which is copyrighted so that one can't incorporate its programming into anything one may be developing.

- **Hacking:** The unauthorized attempt or entry into any other computer system.

- **Internet:** A world wide computer network through which you can send a letter, chat to people electronically or search for information on almost any subject you can think of. Quite simply it is a "network of computer networks".

- **Internet Browser:** An application that displays HTML and other information found on the Internet. Internet Explorer is an example of an Internet Browser. This type of client software accesses the World Wide Web and Gopher services and lets you drift from link to link without having to have a purposeful search.

- **LDM :** Lejweleputswa District Municipality.

- **Public Record:** Includes all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body. Records which contain names or other personally identifying details regarding the users of public, private, school college, university etc.

- **Public resource:** Includes not only LDM equipment, hardware, software or tangible articles, but also the employee's time expended while on duty with the LDM.

- **Risk:** Those factors that could affect confidentiality, availability, and integrity of the LDM's key information assets and systems. The LDM is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

- **Shareware:** Software that is distributed free on a “trial basis” with the understanding that the User my need to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date. Other shareware (sometimes called liteware) is offered with certain capabilities disabled as and enticement to buy the complete version of the program.

- **Third-party:** Any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. A third-party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and trainers.

- **Users:** Any individual who has access to our information systems for the purpose of performing work. Users consist of, but are not limited to: employees, Councilors, third parties etc.

- **World Wide Web (WWW):** A hypertext-based distributed information system for linking databases, servers, and pages of information available across the Internet.

3. Introduction

In order to maximize the benefits of the Information Technology investments of Lejweleputswa District Municipality (LDM), this Technology Usage Policy was created as a way to address all ITC related issues.

This policy requires that all new and existing employees sign a written statement that they have read this policy and understand these guidelines.

4. Objectives

The objective of IT security management practices is to defend all of the components of an information system owned by Lejweleputswa District Municipality, specifically data, software applications, hardware and networks.

5. Communication

The INFORMATION COMMUNICATION TECHNOLOGY UNIT will update this policy, as needed, and submitted the amendments through the normal channels for approval.

6. Standards

The INFORMATION COMMUNICATION TECHNOLOGY UNIT has the responsibility for support and problem resolution for LDM PC's. To effectively carry out that role, the INFORMATION COMMUNICATION TECHNOLOGY UNIT must be able to rely on standard hardware and software configuration on the desktop and notebook computers. Users must request hardware and software through the INFORMATION COMMUNICATION TECHNOLOGY UNIT.

6.1 Hardware Standards

The current hardware for use at LDM is with the INFORMATION COMMUNICATION TECHNOLOGY UNIT. Unit Heads who have a need to deviate from the standards must request an exception. The Municipal Manager will review the request and either approve request as is, or suggest alternate solution to ensure support can be provided.

6.2 Software Standards

The INFORMATION COMMUNICATION TECHNOLOGY UNIT must first acquire and test programs, before it is utilized on LDMs computers. Software may only be used in compliance with the terms of the applicable license agreements.

6.3 Unauthorized Software

Use of unauthorized software can degrade LDM's network and Internet service, create security risks and personal computer problems, divert focus from LDM-related issues, reduce employee productivity and increase costs. It is the responsibility of all Users in all Units as well as Council to comply with maintaining LDM standard by NOT downloading or installing unauthorized software on LDM owned computers. Any software which needs to be downloaded and installed is to be done by the INFORMATION COMMUNICATION

TECHNOLOGY UNIT. Unauthorized software is any software that is not approved for use by the INFORMATION COMMUNICATION TECHNOLOGY UNIT to conduct the business of LDM.

The INFORMATION COMMUNICATION TECHNOLOGY UNIT will:

- Immediately remove the unauthorized software in use when encountered.
- On a routine basis, check and remove unauthorized software, unless the software has legitimate business purpose for the User. The INFORMATION COMMUNICATION TECHNOLOGY UNIT will work with User Units to ensure any questionable software usage is addressed before removal.

7. Network Resource Usage – Internet, E-mail & Data

Access to and use of the network, Internet and/or e-mail systems is provided to employees and Council of LDM for the purpose of advancing the goals of the LDM. This access imposes certain responsibilities and obligations on LDM employees/Council, (full-time, part-time and temporary) as well as any other companies or individuals (third parties) contracted to do work for the LDM, or use LDM IT resources, and is subject to the LDM policies. All data, e-mails, e-mail attachments, documents, and other electronic information within the network/e-mail system are the property of LDM. THERE SHOULD BE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY IN NETWORK USE, AND E-MAIL USE ON THE LDM'S SYSTEMS. The LDM, acting through its managers and supervisors, has the capability and the right to view data and e-mail at any time when deemed necessary for LDM business purposes.

The primary purpose for using the LDM's network, Internet and e-mail connection is in by advancing the business of the LDM. This includes, but is not limited to:

- Communication with, and providing services to, clients of the LDM
- Conducting the business of Units of units
- Communicating with other employees/Council for work-related purposes
- Gathering information relevant to duties or expansion of expertise

Acceptable use always is lawful, ethical, reflects honesty, and shows restraint in the consumption of shared resources. Users shall refrain from monopolizing systems, overloading networks or computers with excessive data (e.g. music/video files) or wasting computer time, connect time, disk space, printer paper, manuals or other resources. Users may be subject to limitations on their use of the networks, or other action, as determined by the appropriate supervising authority. Users are also expected to cooperate with any investigation regarding the use of computers or activities associated with IT resources.

Content of all communications should be accurate. Users should use the same care in drafting e-mail and other electronic as they would for any other written communication. Anything created on the computer may, and likely will, be reviewed by others.

As with internal e-mail messages, internal e-mail can be changed by outside parties and forwarded to others without the employees' knowledge or permission. Users must use caution in using Internet e-mail and must comply with laws.

Recovery of data stored on desktops is the Users' responsibility. Storage only on a PC hard drive is a risk in that if the hard drive fails, the data may not be recovered.

7.1 Limited Personal Use

Authorized Users of LDM may also use the Internet and e-mail for limited personal use. This is defined as any personally initiated online activity (including e-mail and Internet usage) that is conducted for purposes other than those listed above. **This is a privilege**, not a right, and may be limited or removed at any time by management. LDM does not accept any liability for any loss or damage suffered by an employee as a result of that employee using the LDM Internet connection for personal use. Occasional, limited, appropriate personal use of the computer system is permitted when the use does not:

- Interfere with the User's work performance (it shall be infrequent and brief);
- Interfere with the normal operation of the Unit or work unit;
- Interfere with any other User's work performance or have a negative impact on overall employee productivity;
- Have undue impact on the operation of the computer system;
- Cause any additional expense or load to the LDM or Unit;
- Compromise your Unit or the LDM in any way;
- Violate any other provision of this policy, any other policy guidelines.

In limiting personal use, the LDM expects employees to exercise the same good judgment that they would use in all work situations. For example, you are expected to know that taking five minutes to call your spouse during a coffee break is acceptable, while taking three hours to go shopping at the mall during the workday is not. Making decisions about your use of Internet resources is no different. The examples below illustrate the kinds of situations where it is hoped employees would exercise good judgment. Examples provided below are not meant to be exclusive and are for illustration only:

Limited Personal Use	Access Abuse
Dorothy keeps in touch with a circle of friends from school via e-mail. Occasionally she will take a few minutes to read and respond to an e-mail from one of those friends.	John is the convener of a local amateur sports association. He has given his work e-mail out as his main contact. During the sports season, he spends up to 90 minutes each morning responding to queries and complaints, and otherwise conducting league business.
Nauman is a big fan of international soccer. During the World Cup, he takes a few minutes every morning to check a Web site that carries the overnight scores from Europe.	Mike frequents Web sites that are clearly prohibited by the LDM's acceptable policy. Co-workers have been offended by some images clearly displayed on Mike's computer.
Mary reads a review in a magazine of a new novel by Stephen King. While at work the next day, she logs onto Amazon.com and purchases the book for delivery to her home address. She also uses her own personal credit card for the transaction.	James needs a new car and spends over an hour browsing different manufacturers and models.

7.2 Inappropriate Use

The use of public resources for personal gain and/or excessive private use, such as but not limited to the items listed below, by any User is absolutely prohibited and punishable by applicable LDM disciplinary procedures, which may include termination and/or criminal prosecution depending upon the nature and severity of the transgression. The term public resource as used in this policy includes not only the unauthorized use of equipment, hardware, software or tangible articles, but also the employee time expended in the engagement of the unauthorized use while on LDM time.

Examples of unauthorized use of software include streaming music (listening to online radio), stock tickers, news reels, etc., to the desktop, movie downloads, games, screensavers used from the Internet.

Employees may not:

- Use IT resources for personal gain, or to support or advocate for non-LDM related business.
- Create, distribute, upload or download any disruptive, abusive, harassing, threatening, or offensive messages, including offensive comments or graphics about sex, race, gender, colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
- Use IT resources, but not limited to, illegal or unlawful purposes or to support or assist such purposes.
- Attempt to circumvent or subvert system or network security measures, provide internal network access to any non-Users or use your account to gain unauthorized access to external networks and systems.
- Mount an attack on the security of any system (i.e. attempting to hack or introduce viruses into a system).
- Use the network to disrupt network Users, services or equipment. Disrupt include, but are not limited to, distribution of unsolicited advertising, propagation of computer “worms” and viruses, and sustained high volume network traffic that substantially hinders others in their use of the network.
- Intercept network traffic for any purpose unless engaged in authorized network administrative duties.
- Install or use encryption software on any LDM computers without first obtaining written permission from your Unit Head and INFORMATION COMMUNICATION TECHNOLOGY UNIT. Users may not use encryption keys or encryption passwords that are unknown to their Unit Head.
- Engage in online fundraising.
- Mass-mailing LDM-wide messages without approval from the Unit Head.
- Send LDM-wide mailings about viruses, or other warnings about outside computer attacks (these are almost always a hoax, and should be turned over to INFORMATION COMMUNICATION TECHNOLOGY UNIT for disposition).
- Initiate or forward chain letters by e-mail.
- Spoof (disguise) your identity or send anonymous e-mails or send e-mail under another employee’s name without permission.

- Download any non-standard or non-business related files or software, including “freeware” and/or “shareware” programs unless previously approved.
- Load personal Internet Service Provider accounts (i.e. MWEB, Intekom etc.) on LDM owned equipment.
- Unless expressly authorized, sending transmitting, or otherwise disseminating proprietary data, or other confidential information of the LDM is strictly prohibited.
- Make or use illegal copies of copyrighted software or other mediums, store such copies on LDM systems, or transmit them over the LDM network.

It is the responsibility of the supervisor, manager and/or Unit Head to be aware of how the LDM’s Internet facility is being utilized by his/her employees and ensure that employees are periodically informed and aware of the IT policies at a minimum on an annual basis.

7.3 Network Monitoring

All computer applications, programs, data and work-related information created or stored by LDM employees on LDM information systems and resources are the property of LDM. LDM employees shall have no expectation of privacy in anything they store, send or receive on the LDM computer systems. LDM may monitor messages or data without prior notice. LDM is not obligated to monitor e-mail messages. LDM reserves the right to access and monitor e-mail use and any other computer related transmissions, as well as stored information, created or received by LDM Users with LDM Information Technology systems and resources under the following circumstances:

- Performance monitoring and problem solving purposes
- Necessary in the course of an investigation for possible violation of LDM policies
- There is reasonable suspicion that a User has committed, or is committing a crime against the LDM or for which the LDM could be liable
- Random or automated monitoring to ensure that content is in compliance with the business’s established policies
- Request for monitoring is made by appropriate authority
- Required to do so by law

The reservation of this right is to ensure that public resources are not being wasted and to ensure the LDM’s information systems are operating as efficiently as possible in order to protect the public’s interests. This includes blocking access to certain Web sites for which access is deemed to be in conflict with LDM policy.

7.4 E-mail Records Retention

E-mails and attached documents are the property of the LDM, and are subject to LDM rules stated in this policy. Generally speaking, e-mail messages represent

temporary communications that are non-vital and may be discarded routinely. As a result, the e-mail system should not be used to transmit sensitive materials (for example, personnel matters) that may more appropriately be communicated by written memorandum or personal conversation.

However, depending on the content of the e-mail message, it may be considered a more formal record and need to be retained pursuant to a Unit's record retention schedule. Examples of this include policy, decision-making, connected to specific case files, contract related or otherwise an essential part of a larger record, or other memorandum of significant public business.

Managers and supervisors may, with Unit Head approval, access, as necessary, an employee's e-mail if employees are on leave of absence.

8. Security

The LDM has a comprehensive computing environment that encompasses a broad array of networking, server and client computing platforms as well as the complimentary systems software. Users should never consider electronic communications to be either private or secure. E-mail and data could potentially be stored indefinitely on any number of computers, in addition to that of the recipient. Copies of e-mail messages or altered messages may be forwarded to others either electronically or on paper. In addition, e-mail sent to nonexistent or incorrect user names may be delivered to persons that the sender never intended.

Each User is responsible for ensuring that his or her use of outside computer and networks, such as the Internet, does not compromise the security of the LDM network. This duty includes taking reasonable precautions to prevent others from accessing the LDM's network without authorization and to prevent introduction and spread of viruses.

8.1 Network / Internet Security

Standards and requirements exist to ensure security and availability of the data and systems. The LDM's network connects to the Internet through a firewall.

Network Devices – Prior approval from INFORMATION COMMUNICATION TECHNOLOGY UNIT must be obtained before any of the following activities are attempted. These are not allowed by default:

- Connecting any networking devices to the LDM network.
- Usage of modems on individual servers / computers for remote access purposes.
- Allowing non-LDM agencies or entities to access the LDM network without prior INFORMATION COMMUNICATION TECHNOLOGY UNIT approval.

The following activities should only be carried out by INFORMATION COMMUNICATION TECHNOLOGY UNIT or its authorized designees:

- Connecting networking devices to the LDM network
- Interconnecting external networks by routers

To maintain the security of the LDM network, all the Users should ensure that:

- Their PC's have the most current virus protection installed
- Operating systems has all the recommended patches installed
- Browsers have all the recommended patches installed

8.2 Anti-Virus Protection

The LDM network is protected from viruses with the help of firewalls, e-mail scanning software and desktop scanning software, however Users will still be vulnerable to viruses if the following guidelines are not followed.

In some cases, simply reading an e-mail can spread a virus to a User's computer, and from there to many other internal and external LDM recipients. The LDM has taken prudent measures to scan incoming and outgoing e-mail and attempt to intercept viruses. However, no safeguard is foolproof, and viruses can find their way into LDM Users' computers from a variety of other ways (e.g., diskettes from other computers, internet file transfer etc.). Each User is responsible for taking reasonable precautions to avoid introducing viruses into the LDM network.

- NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by deleting them from "Deleted Items"
- Delete and never forward spam, chain, and other junk e-mail
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so
- Always scan a floppy (stiffy) diskette from an external or unknown source for viruses before using it

Viruses and Laptops / Notebooks

Viruses can gain back door entry via laptops (notebooks) that are normally outside the network and which may get infected. To eliminate such risks, the following guidelines should be used while using laptops on the LDM network:

- LDM provided laptops should have "Symantec Antivirus Corporate Edition" software on them. If not present, please inform INFORMATION COMMUNICATION TECHNOLOGY UNIT

- If connected to the LDM network, the antivirus signature for the software is updated daily. All other LDM laptop Users should ensure that they periodically securely connect the laptops and log on to the LDM network for a sustained period of time to get the signature updates.

It is desired that non-LDM laptops not be connected to the LDM network. If it is totally unavoidable then you should:

- Ensure that the laptop has antivirus software loaded on it
- The signature file for the antivirus software is current
- The laptop is scanned for viruses just before it is connected to the LDM network.

Following these steps while using your laptop will help ensure the safety and security of the LDM data and network.

E-mail Scanning

In order to provide further protection for all LDM Users, INFORMATION COMMUNICATION TECHNOLOGY UNIT has implemented additional measures for electronic scanning of incoming and outgoing e-mail. All e-mail attachments coming to the LDM will be electronically scanned for key words that are either sexually explicit, or contain known phrases indicative of spam, hoaxes or viruses. Also, the “Subject” line in e-mail will be scanned for the same kind of key words. Any e-mail with words or phrases matching the key word list will be saved in a quarantine file and a copy of the header information will be sent to INFORMATION COMMUNICATION TECHNOLOGY UNIT who will contact you regarding the rejected e-mail.

It is important to note that e-mail scanning is an electronic comparison to a table of inappropriate words and phrases. This electronic scan will reduce offensive material and make it much more difficult for purveyors of junk e-mail or viruses to interfere with normal operations.

8.3 ID’s and Passwords

Passwords are an important aspect of computer / network security. They are the front line of protection for User accounts. A poorly chosen password may result in the compromise of the LDM’s entire corporate network. The scope of this policy includes all personnel, council, third parties, who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any LDM facility, has access to the LDM network, or stores any LDM information. As such, all are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Users are responsible for safeguarding their passwords for access to the computer systems. Users are responsible for all transactions made using their passwords. No User may access the computer systems using another User’s password or account or portray oneself as another User.

In order to provide appropriate network security, this policy mandates that LDM INFORMATION COMMUNICATION TECHNOLOGY UNIT to utilize passwords and periodically require Users to select a new password, one that they have not used before. Although Users have confidential passwords, this should **NOT** be construed to mean that the application data is the property right of the User or that network, Internet or e-mail access is for personal confidential communications or that the password is to protect the employee's privacy. Users are expected to follow these guidelines when choosing passwords:

- Passwords shall remain confidential and should not be printed, stored online or given to others.
- Passwords shall be changed every 90 days
- Passwords shall be at least six characters long
- Passwords shall contain characters from at least two of the following three classes: (i) English upper / lower case letters, A, a, B, b, (ii) Westernised Arabic numerals, 0, 1, 2 and (iii) Non-alphanumeric ("special characters"), %, &, $
- Passwords may not contain your User name or any part of your full name
- Passwords must not be inserted into e-mail messages or any other form of electronic communication
- The password shall not be found in a dictionary
- The passwords shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters etc.
- The password shall not be your birthday or other personal information such as address and phone number
- The password shall not be a computer term, name, command or site, company, hardware, or software name
- The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc.
- The password shall not be any of the above spelled backwards

8.4 Third-Party Access

A third-party is any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. A third-party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, trainers and auditors.

The policy addresses access to the LDM network and to our information systems. Contractors or other third parties who violate this policy may have their contract revoked. Other legal remedies, including criminal prosecution, may also be pursued if warranted.

8.5 Desktop Security

Please follow the guidelines below to avoid security breaches:

- Store notebooks and personal affects in a locked drawer, file cabinet, or take them away from desk for extended periods of time, including overnight.
- Lock file cabinets when away from desk for extended periods. Do not leave keys in their locks.
- Close applications, and turn off your monitor when you leave your desk.
- Do not leave portable media such as CDs or floppy disks in drives.
- Flash disks can contain lots of confidential information, so do lot leave them lying around.
- Turn off your computer when you leave for extended periods.
- Never write your passwords on a sticky note nor try to hide them anywhere in your office.
- Remove printouts from printers before leaving the office.

8.6 Modem Use Policy

The LDM has spent considerable money and efforts to secure the network. Modems communication is allowed only to certain officials and only to transact LDM business. It is the objective of the LDM to balance the LDM's need for network security and the employee's need for modem communications, prevent outside computer hackers and viruses from destroying computer data both on the network and on PC's and to prevent unauthorized access into LDM computers and data files.

8.7 Portable Memory

The use of USB flash drives, small keychain-sized storage devices capable of holding up to 1GB of data or more, may be useful and practical under certain circumstances, the unchecked usage of them could pose a data security breach, therefore use of them at the LDM is discouraged and requires INFORMATION COMMUNICATION TECHNOLOGY UNIT approval.

Most memory devices of this type are activated simply by plugging them into a USB port, which almost every computer has. From a hardware standpoint, there is nothing to stop unwanted eyes from viewing information on a found or stolen device. Usage of these devices may also cause Users to not utilize the device's native security or backup features (if the device has any, which most don't)

Other drawbacks and negative aspects of portable memory devices such as USB flash drives include, but are not limited to, the following areas of concern:

Theft Sensitive or confidential information could be loaded onto the device via a USB port, leaving no record or trace behind.

Loss Memory devices are small and prone to physical loss, resulting in lost productivity, sensitive data, and so on.

Productivity Lost, destroyed, or stolen data must be retrieved by INFORMATION COMMUNICATION TECHNOLOGY UNIT from

tape backups. Other overhead includes reduced employee productivity from missing data.

Liability A breach in data confidentiality can create severe legal, financial, and HR implications for the enterprise.

Virus While a less likely scenario, an intruder could load a virus or Trojan horse into your network via an open, unattended computer.

Control Users could load illegal copies of software onto their PCs, thus negating normal network defences and leaving the LDM exposed to litigation and damage.

Network Unauthorized downloading and uploading of information to and from memory devices could degrade network performance, stability, and reliability.

8.8 Computer Data Backup

For the Domain server, the following backup policy is administered:

- **Daily Backup:** Every Monday to Friday at around 16:15 a full backup of the Financial and Domain server with all stored information as well as system state and system files are made.

- **Monthly Backup:** Every last Friday of every month at around 16:15 a full backup of the financial server with all stored information as well as system state and system files is made.

- **Yearly Backup:** The yearly backup occurs on the last working day of the year and a full backup of the financial server with all stored information as well as system state and system files are made.

- **Retention Policy:** Daily backups are valid for one full week. Monthly backups are valid for one full year, whereas yearly backups are kept eternally or until disposed of by order.

8.9 Security Access Removal

Computer System Security: Removal of an employee's computer access account is used when and employee leaves the LDM. The Unit Head or authorized designee must inform the INFORMATION COMMUNICATION TECHNOLOGY UNIT and also make the necessary arrangements regarding e-mail and information that might still be stored on the LDM Domain server. Otherwise, any and all data associated with the account will be deleted.

Laid-off or terminated employees have no right to the contents of their e-mail messages or data stored in LDM systems, and should not be allowed access to the computer systems. Should an employee be suspended from duty, will the User's access account be frozen until the suspension has been lifted.

9. Policy Infraction

LDM employees as well as LDM Councillors who violate this policy may have their access removed and may be subject to disciplinary action up to and possibly including termination. In addition, contractors or other third parties who violate this policy may have their contract revoked. Other legal remedies, including criminal prosecution, may also be pursued if warranted.

Sanctions for inappropriate use of LDM network resources or failure to comply with this policy may include, but are not limited to, one or more of the following:

- Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
- Disciplinary action according to applicable policies and regulations;
- Legal action according to applicable legislation and contractual agreements.

The rules and guidelines require strict adherence. Failure to conform and comply with these rules and guidelines will subject individuals to appropriate disciplinary action commensurate with the severity of the infraction and may result in disciplinary actions up to and including termination as well as criminal prosecution.

10. Computer Support / Technology Requests

10.1 Computer Support

The Information Communications Technology Unit offers support for existing LDM computer systems. This includes support to all LDM computer hardware as well as approved software. No support will be given to unauthorized software or games. Users should supply symptoms or error codes of specific problems when logging calls to the INFORMATION COMMUNICATION TECHNOLOGY UNIT. No User shall log calls directly to third-parties or contractors.

10.2 Technology Requests

All requests for new technology or the possible upgrading of current technology shall be made in writing to the INFORMATION COMMUNICATION TECHNOLOGY UNIT. All requests shall be accompanied with the vote the technology is requested for. The INFORMATION COMMUNICATION TECHNOLOGY UNIT shall do the necessary research on the requested technology.

All newly purchased technology shall be received, checked, recorded and installed by the INFORMATION COMMUNICATION TECHNOLOGY UNIT. No technology shall be installed by any other employees, contractors or any third-parties.

11. Computer Training

Computer training is beyond the scope of this policy as it is an HR function. It is recommended though that all intended ICT training be discussed with the INFORMATION COMMUNICATION TECHNOLOGY UNIT.