**TECHNOLOGY USAGE POLICY**

|  |
| --- |
| **DOCUMENT DETAILS** |
| **Document Name:** | Technology Usage Policy | **Document No:** |  |
| **Department Name:** | Human Resources | **Document Type:** | Policy |
| **UPDATE DETAILS** |
| **Last Updated:** |  | **Updated By:** |  |
| **Effective Date:** |  | **Approved By:** |  |
| **Approval Date:** |  | **Approved By:** |  |
| **Revision Date:** |  | **Approved By:** |  |

**PURPOSE:**

We provide our employees with the best tools possible so as to remain competitive and better serve our customers. [YOUR COMPANY NAME] (“the Company”) makes available to all employees one or more forms of electronic media and services, including but not limited to: software, computers, copier, printers, files, cellular phones, email, databases, online services, voicemail, internet and intranet.

The purpose of providing all employees and everyone connected with the organisation with access to the electronic media and other technical devices is to assist and support company business. Employees are reminded that all these devices and electronic media is the property of [YOUR COMPANY NAME] and should be used in a respectful, professional and ethical manner.

The following guidelines are to be followed by all employees for using email and the internet. It is impossible for us to cover all and every situation that might occur in one policy document, it is instead designed to express [YOUR COMPANY NAME] philosophy and set forth general principles when using electronic media and services.

**SCOPE:**

This policy applies to all employees of the ............................

**RESPONSIBLE PERSONS:**

1. HR Manager - Implementation and facilitation.
2. IT Manager - Administration, monitoring and enforcement of this policy.
3. Employees - Adherence to this policy and procedures outlined in this policy.

**POLICY STATEMENT:**

It is agreed between management and employees that this policy is not a unilateral change in the employment conditions of the employees of this company; and that the implementation of this policy is as a result of the required alignment of policies within the .........................

**GENERAL OBLIGATIONS OF THE EMPLOYEE:**

In order to effectively manage this Technology Usage procedure, all employees shall ensure their access and adherence thereto.

**TECHNOLOGY USAGE:**

1. **AUTHORIZATION**

Access to the [YOUR COMPANY NAME] technology resources is within the sole discretion of Management. Employees will be given access to the Company’s different technologies based on their job description. If the employees job performance benefits form the use of the technology resources then it will be provided and access will be granted. Additionally, employees must undergo and complete basic company training before access will be granted to the technology resources.

1. **PROHIBITED COMMUNICATIONS**

Employees may not use the electronic media to knowingly transmit, copy, retrieve or store any communication that is:

* Harassing or discriminatory;
* Derogatory to any individual or group;
* Pornographic, explicit, obscene, sexual, threatening or defamatory;
* In violation of any licence governing the use of the software;
* Engaged in for any reason that is illicit or as opposed to [YOUR COMPANY NAME] approach, in any capacity that unveils private or restrictive data of the company or outsiders, or for individual or monetary gain.
* Unless an employee has the permission from the author or is only accessing a copy for his personal records, all data is protected by copyright laws.
1. **PROFESSIONAL CONSIDERATIONS**

It is imperative that all employees conduct themselves with the correct tone to their communications over the system. The following guidelines have been set out to assist:

* Make your communications constructive, positive, complete and factual.
* Don’t write when you are angry
* All documents must be edited before sent.
* Be aware of using humour – they can’t see you wink.
* Never use sarcastic humour.
* Do not use all caps – that is perceived as “SHOUTING!”
* Always guide your recipient *in re*sponding by stating what you need and by when.
* To protect your own reputation and intelligence, always pay attention to grammar and spelling.
1. **PERSONAL USE**

The computers, electronic media and services provided by [YOUR COMPANY NAME]are primarily for business use to assist employees in the performance of their jobs. As long as personal use does not interfere with the employee's duties, is not done for pecuniary gain, does not conflict with the Company's business, and does not violate any Company policy, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

The Company assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted over or stored on the Company's technology resources. The Company accepts no responsibility or liability for the loss or non-delivery of any personal electronic mail or voicemail communications or any personal data stored on any Company property. The Company strongly discourages employees from storing any personal data on any of the Company's technology resources.

1. **ACCESS TO EMPLOYEE COMMUNICATIONS**
	1. Generally, electronic information created and/or communicated by an employee using email, word processing, utility programs, spreadsheets, voicemail, telephones, Internet and bulletin board system access, and similar electronic media is not reviewed by the company. However, the following conditions should be noted:

[YOUR COMPANY NAME] does routinely gather logs for most electronic activities or monitor employee communications directly, be it:

1. **Telephone Use and Voicemail:** Records are kept of all calls made from and to a given telephone extension. Although voicemail is password protected, an authorised administrator can reset the password and listen to voicemail messages.
2. **Electronic Mail:** Electronic mail is backed-up and archived. Although electronic mail is password protected, an authorised administrator can reset the password and read electronic mail.
3. **Desktop Facsimile Use:** Copies of all facsimile transmissions sent and received are maintained in the facsimile server.
4. **Document Use:** Each document stored on Company computers has a history, which shows which users have accessed the document for any purpose.
5. **Internet Use:** Internet sites visited, the number of times visited, and the total time connected to each site is recorded and periodically monitored.

[YOUR COMPANY NAME] reserves the right, at its discretion and without notice, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other company policies, or to investigate misconduct, to locate information, or for any other business purpose.

* 1. Employees should understand, therefore, that they have no right of privacy with respect to any messages or information created or maintained on the Company's technology resources, including personal information or messages. Accordingly, if they have sensitive information to transmit, they should use other means.

All messages sent and received, including personal messages, and all data and information stored on the Company's electronic-mail system, voicemail system, or computer systems are Company property regardless of the content. As such, the Company reserves the right to access all of its technology resources including its computers, voicemail, and electronic-mail systems, at any time, in its sole discretion.

Passwords do not confer any right of privacy upon any employee of the Company. Employees are expected to maintain their passwords as confidential. Employees must not share passwords and must not access coworkers' systems without express authorization.

Deleting or erasing information, documents, or messages maintained on the Company's technology resources is, in most cases, ineffective. All employees should understand that any information kept on the Company's technology resources may be electronically recalled or recreated regardless of whether it may have been "deleted" or "erased" by an employee. Because the Company periodically backs-up all files and messages, and because of the way in which computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information or messages are confidential.

1. **THE INTERNET AND ON-LINE SERVICES**

The Company provides authorised employees access to on-line services such as the Internet. The Company expects that employees will use these services in a responsible way and for business-related purposes only. Under no circumstances are employees permitted to use the Company's Technology Resources to access, download, or contribute to the following:

* gross, indecent, or sexually-oriented materials;
* sports sites;
* job-search sites;
* entertainment sites;
* gambling sites;
* games, humor;
* illegal drug-oriented sites;
* personal pages of individuals; and
* politically-oriented sites or sites devoted to influencing the course of legislation or public policy.

Additionally, employees must not sign "guest books" at Websites or post messages to Internet news groups or discussion groups at Websites. These actions will generate junk electronic mail and may expose the Company to liability or unwanted attention because of comments that employees may make. The Company strongly encourages employees who wish to access the Internet for non-work-related activities to get their own personal Internet access accounts.

1. **PARTICIPATION IN ONLINE FORUMS**
	1. Employees should remember that any messages or information sent on company-provided facilities to one or more individuals via an electronic network – for example, Internet mailing lists, bulletin boards, and online services – are statements identifiable and attributable to [YOUR COMPANY NAME].
	2. [YOUR COMPANY NAME] recognises that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a news group devoted to the technical area.
2. **SOFTWARE**

To prevent computer viruses from being transmitted through the company's computer system, unauthorised downloading of any unauthorised software is strictly prohibited. Only software registered through [YOUR COMPANY NAME] may be downloaded. No employee may load any software on the Company's computers, by any means of transmission, unless authorised in advance by [YOUR COMPANY NAME]’s system administrator.

1. **SECURITY/APPROPRIATE USE**
	1. Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by company management, employees are prohibited from engaging in, or attempting to engage in:
* Monitoring or intercepting the files or electronic communications of other employees or third parties;
* Hacking or obtaining access to systems or accounts they are not authorised to use;
* Using other people's log-ins or passwords; and
* Breaching, testing, or monitoring computer or network security measures.
	1. No email or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.
	2. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
	3. Anyone obtaining electronic assess to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.
	4. The Company has installed a variety of programmes and devices to ensure the safety and security of the Company's technology resources. Any employee found tampering or disabling any of the Company's security devices will be subject to discipline up to and including termination.
1. **ENCRYPTION**

Employees can use encryption software supplied to them by the systems administrator for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a company computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

1. **CONFIDENTIAL INFORMATION**

The Company is very sensitive to the issue of protection of trade secrets and other confidential and proprietary information of both the Company and third parties ("Confidential Information"). Therefore, employees are expected to use good judgement  and to adhere to the highest ethical standards when using or transmitting Confidential Information on the Company's technology resources.

Confidential Information should not be accessed through the Company's technology resources in the presence of unauthorised individuals. Similarly, Confidential Informa­tion should not be left visible or unattended. Moreover, any Confidential Information transmitted via technology resources should be marked with the following confidentiality legend:

"This message contains confidential information. Unless you are the addressee (or authorised to receive for the addressee), you may not copy, use, or distribute this information. If you have received this message in error, please advise [EMPLOYEE'S NAME] immediately at [EMPLOYEE'S TELEPHONE NUMBER] or return it promptly by mail."

1. **VIOLATIONS**

Any employee who abuses the privilege of their access to email or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

1. **PROCEDURES**

Procedures for accessing the Voicemail, Email and Internet system, as well as the guidelines for how to properly send and retain information, may be obtained by contacting [NAME OF THE SYSTEMS ADMINISTRATOR].

The Voicemail/Email/Internet policies and procedures should be reviewed by each employee on a semi-annual basis.

Questions concerning the use of the Voicemail/Email/Internet system should be directed to the systems administrator. Questions concerning the improper use of the system should be directed to the employee’s immediate supervisor, and if not satisfied with the response, to the systems administrator.

1. **EMPLOYEE AGREEMENT ON USE OF EMAIL AND THE INTERNET**

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of the Company's computer and telecommunications equipment and services. I understand that I have no expectation of privacy when I use any of the telecommunication equipment or services. I am aware that violations of this guideline on appropriate use of the email and Internet systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of the email and Internet may reflect on the image of [YOUR COMPANY NAME] to our customers, competitors and suppliers and that I have responsibility to maintain a positive representation of the company. Furthermore, I understand that this policy can be amended at any time.

**TECHNOLOGY INFO FORM**

A separate technology form must be completed for each step of the grievance procedure.

|  |
| --- |
| **TECHNOLOGY INFO FORM** |
| Employee Name/s: |  No/s: |
|  |  |
| Department: | Job Title: |
| HARDWARE EQUIPMENT ISSUES:Desktop ComputerLaptop ComputerTablet/IpadCellphone | 🞎🞎🞎🞎 |
| OTHER:Email address:Computer Password:Other: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Notes: |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Signature of employee: | Date: |
| Signature of manager: |  Date: |
|  |  |
|  |  |

* **DOCUMENTS MENTIONED AND TO BE USED IN ENFORCING THIS POLICY**

TECHNOLOGY INFORMATION FORM

**EMPLOYEE POLICY CONFIRMATION:**

***I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (employee name and surname), declare that;***

1. Ihave been familiarised with and informed of the Technology Usage Policy.
2. I understand and agree to the contents of this policy and that;
* it may be amended from time to time,
* it forms part of my employment conditions,
* the implementation and contents of this policy are mutually agreed upon with the employer,
* I have been given the opportunity to question this policy and that my questions were satisfactorily answered
1. I agree to strictly adhere to this policy.

Signed at \_\_\_\_\_\_\_\_\_\_\_\_ (place) on the \_\_\_\_\_\_\_\_\_\_ of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [YEAR].

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Employee

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Manager