**Information Technology, Email and Internet Policy**

# Policy Statement

All Employees are required to adhere to **(Insert Organisation Name)** policies and procedures which reflect the behaviour expected and is designed to encourage integrity and professionalism.

The **Information Technology, Email and Internet Policy** are a set of guidelines for which all employees are expected to observe and adhere to.

This policy forms part of all employees of **(Insert Organisation Name)** employment conditions.

**Sources**

* Grievance Policy
* Work Health & Safety Policy
* Staff Handbook
* Fair Work Act 2009
* Fair Work Regulations 2009

**Application of this Policy**

This policy applies to all **(Insert Organisation Name)** employees and volunteers.

**Responsibility for Implementation**

All managers, supervisors, and staff are to ensure they use all computers, laptops, mobile phones or electronic devices in line with this policy. All managers, supervisors, and staff are to ensure they also follow the guidelines when using these devices for email and internet usage.

Any breaches of this policy are to be reported the ***(Insert Position)***.

**(Insert Organisation Name) Responsibilities**

Laptop Computers, Desktop Computers, IPads, Mobile Phones, and mobile devices are supplied to staff of **(Insert Organisation Name).**

All Laptops, Computers are set up to connect to the organisation Network.

Each computer, laptop and other device has been loaded with the latest version of virus scanning software and this updated on a regular basis.

**(Insert Organisation Name)** will continue to maintain up to date and when required computer technology for all staff.

All users must realise when they use the Internet, they are representing **(Insert Organisation Name).**

Employees must be aware of the instantaneous nature of IT related communications; it is easy to inflame professional relationships. The conversational style of email in particular, can lead to your intended message being misinterpreted.

Email and Internet facilities may only be used for business-related communications and purposes. If you view or download material from the Internet other than for business purposes.

An employee must never send confidential or sensitive information through the Internet or email, unless directed.

Do not send certain types of attachments, including pictures, movie clips, programs etc. You should discourage other colleagues from sending these kinds of attachments to you.

All employees need to be aware of the **(Insert Organisation Name),** policies on sexual harassment and workplace harassment apply to the transmission of offensive material either through the Internet or email. The distribution of pornographic or sexually explicit material through the **(Insert Organisation Name)** email or other electronic means will not be tolerated and will be dealt with as a serious disciplinary issue and may result in termination.

Downloads from the Internet or Software

Employees are to ensure if they download from the Internet that the information they are downloading are free from viruses and the material is not to be used for inappropriate purposes.

**Privacy**

All employees’ emails at work are not private and may be reviewed by your employer **(Insert Organisation Name).** While there is no intention to “snoop”, **(Insert Organisation Name)** is legally responsible for all email communications and will review all emails on an ongoing and continuous basis where necessary.

**Legal Issues**

All employees must be aware that emails, unlike telephone calls, create a permanent written record of communications. If in doubt, do not send any email.

Employees should never download material subject to copyright from the Internet, such as computer software. If in doubt ask your supervisor.

**Authorship**

No person may, in any circumstances, send any email in the name of another employee without the other employee’s express permission and unless the action is authorised by your supervisor.

If you access or attempt to access another employee’s email or other computerised records on the organisation computer system without authority, you will breach **(Insert Organisation Name)** security and privacy policies. If an employee accesses another’s employee’s email or computerised records without authorisation, will not be tolerated and will be dealt with as a serious disciplinary action and may result in termination.

**Personal Use**

Employees must not use email for personal or private communications whilst at work. The email and internet system is a business tool intended to be used for work related purposes. **(Insert Organisation Name)** will discipline employees for private email use including sending unsolicited junk email or advertising or copying emails to others. Repeated private use at unacceptable levels will result in termination.

**Housekeeping**

All employees are to check their email regularly. There will be some emails that must be printed and the hard copy kept on file. Employees are to empty their trash box on a daily basis and file or archive on a regularly basis.

**Confirmation**

Ensure that you seek confirmation of receipt for important messages and emails. If the employee does not know how to do this, talk to your Supervisor.

**Email not meant for you**

You must not read, delete, copy or modify an email owned by other users within **(Insert Organisation Name)** without permission. Do not forge electronic mail messages to make them look as though they are coming from another person.

**Respect for others**

All employees must not send obscene, abusive, sexist, racist, or threatening emails. Emails must also not be used for defamatory, offensive or otherwise unwelcome communication, or any communication which is discriminatory or harasses any person. If any of this inappropriate conduct occurs, you may be disciplined or terminated.

**When an employee is absence from work**

When an employee is away their email messages will be checked by their Manager/Supervisor.

When an employee goes on leave, turn on ‘Out of Office’ before you leave and include the appropriate dates that the employee will be away. If necessary re-direct emails to someone else in organisation.

**Software Viruses**

Software viruses are programs designed to make unauthorised changes to programs and data. Therefore, viruses can cause destruction of resources.

The following apply to all staff:-

* Employees shall not knowingly introduce a computer virus onto their work computers/laptop computers.
* Employees shall not load or install software or CD of unknown origin.
* Any employees who suspects that their Computer/Laptop Computer has been infected by a virus shall IMMEDIATELY inform your supervisor or manager.

**Physical Security for Laptop Computers**

The following apply to all staff who have laptop computers:-

* Laptop computer should be stored out of sight when not in use.
* Laptop computer should be kept away from environmental hazards such as heat, direct sunlight, water etc.
* Environmental hazards to Laptop Computers such as food, smoke, liquids, dust, high or low humidity, and extreme heat or cold should be avoided.
* Employees should exercise due care to safeguard the Laptop Computer assigned to them.

**Breaches of Policy**

Non-compliance with this policy and any damage or neglect to IT equipment of **(Insert Organisation Name)** may result in disciplinary action, which could include termination of employment in serious cases. Employees who breach the law may be personally liable for their actions through common law claims.

## Policy Review

The ***Information Technology, Email and Internet Policy*** will be reviewed from time to time, and all staff will be trained, educated and will be required to sign an acknowledgement that they understand and will comply with this policy. Should the need arise; the policies will be translated into appropriate languages.

**(Insert Organisation Name)** is committed to providing an environment which is safe for all who attend or work at its workplaces.

**Employee Acknowledgment - Social Media Policy**

I \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ have been provided with a copy of the **(Insert Organisation Name) Information Technology, Email and Internet Policy**

I have read and understood the material contained within the **Information Technology, Email and Internet Policy**, and I have had the opportunity to ask questions about any of the material set out in that policy.

I understand the ramifications of failure to adhere to the policy.

Sign: Date:

Print Name:

Witness: Date:

Print Name: