# Information Services Acceptable Use Policy for Staff

## Effective: August 2020

## Version: 1.3

Note, this document is available in alternative formats upon request including electronic or audio format.

## Table of Contents

## Policy Statement

This Policy provides a framework that ensures users make appropriate use of the Organisation's IT services and provides information about the consequences of misuse. Inappropriate use exposes the organisation to cybersecurity risks including virus attacks, compromise of network systems and services and legal issues. All users of Organisation IT services are required to comply with the principles outlined in this policy.

## Scope

This policy applies to all users of Organisation IT services (inclusive of but not limited to) employees, contractors, third party service providers or other persons affiliated but not employed by the Organisation. Users of IT services are responsible for exercising good judgement regarding appropriate use of information, electronic devices, and network resources in accordance with the Organisation policies and standards and Australian laws and regulations.

## Principles

The following overarching principles are to be followed by all users with access to Organisation systems or data.

### 1. Business first

IT assets and services are made available to employees for business purposes to perform their duties.  Limited personal use is permitted provided it does not impact the performance of those duties and Organisation operational requirements.

### 2. Protect Organisation interests

IT services should not be used in a way that could cause the organisation embarrassment or loss.

### 3. Approved components

Currently only Organisation authorised equipment, software, and services can be introduced and used in the Organisation's corporate IT environment. Personal devices can be connected to Organisation guest Wi-Fi network. Employees are responsible for the protection of their allocated equipment and software and safeguarding the use of their accounts. Organisation will continue to assess and evaluate the need for a BYOD strategy to facilitate greater collaboration, communication and information access across the Organisation IT environment including integrated cloud solutions.

## 4. Lawful use

Organisation IT assets and resources can only be used for lawful activities and cannot be used for any activities which would contravene any laws or regulations with which the Organisation is obliged to comply with.

## 5. Report issues

Security is everyone's responsibility. The IT Support Helpdesk IT@xxxx.au (extension 333) is to be contacted immediately if employees believe or suspect that something is not secure, require advice or would like to report IT issues such as a security breach.

## 6. Unacceptable use

The following activities are in general, prohibited and deemed unacceptable use. This list is by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use. These activities include, but not limited to the following.

### a. General

Users must not:

- access Organisation information, systems and technology services, data, a server, or an account for any purpose that they have not been authorised to use i.e., not for the purpose of conducting Organisation business even if they have authorised access.

- use another employee's digital identity nor attempt to find out the password of another employee, share or reveal passwords to others, allow the use of their account by others (including family and other household members when working from home) or leave their device unsecured.

- attempt to subvert security measures in any way e.g., undertake any activities that could result or assist in the violation of laws, regulations or Organisation policy including but not limited to copying of copyrighted material, installation, or distribution of unauthorised, 'pirated' or other software products that are not appropriately sanctioned or licensed for use by the Organisation. Examples of these prohibited tools include viruses, Trojan horses, worms, password breakers, network packet observers or sniffers.

- Examples of prohibited activities include creating ping floods; spoofing packets; performing denial-of-service attacks; forging routing information for malicious purposes; scanning for vulnerabilities; or other computer hacking techniques.

- effect security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, 'disruption' includes, but is not limited to network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- undertake port scanning or security scanning unless prior authorisation has been granted by the Chief Information Officer or delegated authority.

- circumvent user authentication or security of any host, network, or account.

- execute any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal duties.

- introduce malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs etc.).

- interfere with or denying service to any user other than the employee's host (for example, denial of service attack).

- introducing honeypots, honeynets, or similar technology on the Organisation network.

- use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

- attempt to adversely interfere with the operation of any of the Organisation IT services. For the purposes of this document, interfering includes wilful physical damage, wilful destruction of information, wilful interruption of normal operations, theft and accessing restricted areas.

- wilfully waste IT services e.g., wasting network bandwidth by downloading, printing, or sending large amounts of material that is not work-related.

- use IT services to send obscene, offensive, bogus, harassing, or illegal messages.

- use IT services for personal commercial benefit nor publish or circulate information about other organisations via IT services.

- use the IT services in a way that would be considered to pose cyber threat or social engineering risk to the Organisation or any other party.

- intentionally create, view, transmit, distribute, copy, or store pornography or objectionable material or any information, data or material that violates Australian legislation (including federal legislation or Western Australian state legislation). For example, you must not view, store, send, or give access to material regarded as objectionable by the Western Australian Classification (Publications, Films and Computer Games) Enforcement Act 1996 No. 40 (e.g., sexually explicit material, incitement to violence, torture, and bestiality).

- attempt to conceal or erase the evidence of a breach of Organisation IT security.

- allow their computer or personal devices to adversely affect Organisation IT services.

- leave personal information stored within Organisation IT services after their contract of employment ceases. Employees must plan for its retention and/or removal as appropriate prior to cessation of their contract.

- export software or technical information, in violation of international, regional, or local export control laws that is illegal.

- undertake unencrypted transfer or storage on removable media of sensitive or confidential information.

- make fraudulent offers of products, items, or services originating from any Organisation account.

- use unauthorised file sharing systems.

- Use software that is not on the Software Register

- provide information about lists of, or photographs of employees to parties outside the Organisation.

- Use the Organisation ICT network for the purpose of copyright infringement.

## b. Inappropriate use of the internet

Users must not:

- Play online games, stream video or radio content, unless it is related to training delivery or their job function.
- Access material of an offensive, obscene, threatening, abusive or defamatory nature unless in a training environment deemed suitable by the lecturer.
- click on ‘pop-up’ sites and/or adverts.

## c. Inappropriate email use

Users must not:

- send unsolicited email messages, including the sending of ‘junk mail’ or other advertising material to individuals who did not specifically request such material (email spam).
- create or forward ‘chain letters’, ‘Ponzi’ or other ‘pyramid’ schemes of any type.
- carry out any form of harassment via email, telephone, or paging, whether through language, frequency, colour or size of messages.
- make unauthorised use or forging of email header information.
- solicit for other email addresses, other than that of the poster’s account, with the intent to harass or to collect replies.
- register a work email address on any non-work-related site e.g., Facebook or Twitter unless approved by a director for training purposes.
- distribute confidential or sensitive material externally to a third party (except for the Department of Training and Workforce Development) without the data custodians’ consent or electronically in an unsecure manner.
- email material which contains viruses, worms, ‘Trojan horses’ or any other contaminating or destructive features.

- redirect, forward, copy or move email containing Organisation business information to personal email addresses.
- social chat with colleagues which is outside of reasonable personal use.

### d. Telecommunication use

Users must not:

- make calls that are offensive, obscene, threatening, abusive or defamatory.
- use telephones and mobiles for personal commercial benefit.
- inappropriately transmit information which may violate the rights of others, including unauthorised text, images or programs, trade secrets, confidential property, or trademarks.
- use telecommunications equipment outside of Australia unless prior approval has been granted by the Managing Director.

## 7. Compliance

To ensure staff compliance with this policy, the Organisation reserves the right to verify compliance to this policy through various means including but not limited to monitoring users of IT service activity and accessing data to ensure acceptable use. This may include but is not limited to reviewing logs, accessing email accounts, and engaging internal and /or external audit. Users acknowledge that their usage may be monitored.

When using organisational resources to access and use the Internet, users must realise they represent the Organisation. Whenever employees state an affiliation to the Organisation, they must also clearly indicate that ‘the opinions expressed are my own and not necessarily those of the Organisation’.

## 8. Non compliance

a) Any employee found to have violated this policy may be subject to disciplinary procedures as outlined in Discipline Policy.

b) the Organisation may terminate an employee’s IT service access and/or notify the relevant authorities if Organisation staff believe that a breach has occurred.

c) Sanctions applied in non-IT areas may result in removal of IT services to the staff member.

## Background

The Organisation is committed to protecting its employees, partners, employees, and the organisation from illegal actions by individuals, either knowingly or unknowingly. IT resources are to be used in a responsible and accountable manner that ensure the efficient, effective, and acceptable use. Additionally, employees are aware that they are bound by the Organisation Code of Conduct which has provisions for the proper use of official information, equipment, and facilities.

The Organisation provides employees with the following IT services for work purposes:

- access to computer software and equipment,
- access to wireless network services,
- access to the Internet,
- access to email,

All IT systems, including but not limited to computer equipment, software, operating systems, storage media and network infrastructure are the property of the Organisation. These systems are to be used for business purposes in serving the interests of the organisation and of our customers in the course of normal business operations.

Effective information security is a team effort involving the participation and support of every staff member who deals with information and/or information systems.

For further information on cyber security, please refer to: https//staysmartline.gov.au.

Under the Criminal Code Act (1995), it is an offence to use the internet, social media, or a telephone to menace, harass or cause offence. The maximum penalty in this offence is a three-year imprisonment or a fine of more than $30,000.

Information on how to report cyber bullying and illegal content can be found on the eSafety Commissioner’s website: https://www.esafety.gov.au.

## Definitions and Acronyms

| Term | Definition |
|---|---|
| Virus | A computer program that can infect other computer applications or system areas by modifying them to include a copy (possibly modified) of itself. |
| BYOD | Bring Your Own Device |
| Malware | Unwanted or malicious software e.g., worms, Trojan horses, bots. |
| Worms | A worm is a program that makes copies of itself (usually one per system) across a network. It may do damage and compromise the security of a computer, but it doesn't replicate by changing a hosts code or files. Viruses infect, worms infest. |
| Trojan horses | A Trojan Horse is a program that does something that its programmer intended but the user is not expecting. Viruses must replicate to be classed as viruses; Trojans do not replicate. |
| Packet sniffers | A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. |
| Ping floods | A ping flood is a simple denial-of-service attack where the attacker overwhelms the victim with Internet Message Control Protocol (ICMP) echo request (ping) packets. |
| Spoofing packets | Involves masking the IP address of a certain computer system. |
| Denial-of-service | A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. |
| Honeypots | A computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. |
| Honey net | A network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated. |

## Related polices and other relevant documents

Staff Code of Conduct

## Related legislation

State Records Act 2000

Freedom of Information Act 1992

## Review Date

November 2023

## Contact Information

Chief Information Officer

## Revision History

| Version No. | Approved/ Amended/ Rescinded | Date | Approval Authority | Amendments |
|---|---|---|---|---|
| 1.2 | Approved | August 2020 | ITC MD | |
| 1.3 | Amended | November 2022 | | Corrected grammar errors |