



## ACCEPTABLE USE POLICY

The Acceptable Use of Information Communication Technology (ICT) Resources Policy (**Acceptable Use Policy**) instructs Mid West Ports Authority (**MWPA**) Directors and Workers in the acceptable use of ICT resources.

This policy applies to all ICT resources, devices and services including:

- desktop computers and devices;
- mobile devices such as laptops, tablets and smartphones provided by MWPA;
- personally owned devices connected to MWPA networks; and
- network, server, storage and cloud resources.

### ACCEPTABLE USE

Acceptable use of MWPA ICT resources is governed by the MWPA Code of Conduct. Directors, and Workers must:

- manage the ICT resources entrusted for use honestly and responsibly;
- avoid excessive personal use of ICT resources; and
- not allow personal use to interfere with user's official duties.

### Official Use

MWPA ICT resources are the property of MWPA and may only be used for lawful purposes and consistent with MWPA values.

Directors and Workers are only permitted to use ICT resources for the performance of their official duties, with reasonable "Personal Use".

### Bring Your Own Device (BYOD)

Personal devices may be used for official use and will be setup by the ICT team.

Where a BYOD is used for work purposes, excessive personal use must not occur during normal working hours.

Approved users must comply with the MWPA Telephone and the Information Security procedures when accessing official information.

### Personal Use

Approved users may make reasonable personal use of MWPA ICT resources, such as instant messaging, streaming media, email and web browsing on the desktop or laptop computer issued, provided it is not prohibited use as defined by this policy.

The access or download of large personal files, unapproved software or saving them to ICT resources is prohibited.

### Security Responsibilities

Workers are responsible for protecting MWPA's information technology resources from unauthorised access, disclosure, alteration, and destruction.

Workers must comply with all applicable laws, regulations, and MWPA's policies regarding Information Security.

MWPA has implemented appropriate data privacy protections to safeguard personal information, sensitive company data, and other confidential information.



## **PROHIBITED USE**

Directors and Workers MUST NOT create, communicate, access, download or store inappropriate or prohibited material using MWPA ICT resources.

Inappropriate and prohibited material includes, but is not all inclusive of, the following:

- text, graphics, video or other material of a sexual nature (including pornography and other adult material such as swimsuit or lingerie modelling).
- offensive language or offensive material, including jokes or commentary of a sensitive nature (e.g. about race, age, gender, disability, marital status, sexual orientation, religion, political beliefs or appearance).
- racially offensive material which, if communicated, would constitute offensive behaviour within the meaning of *Section 18C* of the *Racial Discrimination Act 1975*.
- material that is defamatory, abusive or constitutes a form of unlawful discrimination or potential harassment.
- gambling or financial market trading material.
- dating and chat rooms.
- malicious software.
- criminal skills material including instructions on how to obtain drugs or stolen property or create weapons or explosives.
- create or post to personal blogs or personal web pages; or
- conduct a private online business (including selling on eBay or similar sites or share trading).

ICT resources are not to be used to engage in any conduct that vilifies, harasses or discriminates against a person based on their race, sex, sexual preference or identity, religion or disability.

## **Excessive Use**

Excessive personal use of ICT resources is prohibited, particularly where it impacts on official duties, or on MWPA operational effectiveness, clients, Workers, or resources.

## **Copying or Installing Software**

The installation of software on MWPA ICT resources is prohibited. All software Must be approved by the MWPA ICT Manager and installed by the MWPA ICT team.

## ENFORCEMENT

Any services (including equipment) provided by MWPA may be suspended or terminated with or without notice upon any violation of this policy.

This Policy overrides any previous policy, procedure or agreement, either written or verbal, relating to matters contained within.



Mr Noel Hart

Chair

Date Approved: 20 March 2024

Board Meeting Resolution Number: 24/115/001



Mr Damian Tully

Chief Executive Officer