ACCEPTABLE USE OF IT RESOURCES POLICY

Version No: 1.0 | Author: General Manager ICT | Next Review Date: 2026/01

1. Purpose

1.1. BACKGROUND

Information Technology (IT) resources are vital for delivering services at McKenzie Aged Care Group (MACG). MACG respects the confidentiality and privacy of personal and sensitive information, health information, customer and employee information, or other related information accessible via our systems and environments. MACG is committed to maintaining a safe, reliable, and secure technology environment that allows it to meet its organisational objectives, legal requirements, and ethical responsibilities.

This policy stipulates constraints and practices that users must agree for appropriate use of MACG IT resources including the internet, or other resources authorised for official use.

The purpose of this policy is to:

- establish standards for acceptable use of MACG IT resources and information.
- regulate the access to MACG IT resources; and
- ensure protection of information held within MACG environments.

Permission to use MACG IT resources is contingent upon compliance to this policy. This policy must be reviewed in conjunction with the *MACG Privacy Policy* and *MACG Information Security Policy*.

1.2. SCOPE

This policy applies to:

a) all technology resources used by, operated by, or provided on behalf of MACG;

b) all information collected, created, stored, or processed by, or for MACG on our information systems and infrastructure; and

c) all individuals who utilise, or are involved in deploying and supporting, information systems and resources provided by MACG. This includes all staff (full-time, part-time, casual), contracted and agency staff, students, volunteers, suppliers, partners, contractors, sub-contractors, or affiliated organisations; and

d) all external suppliers contracting with MACG and any of their personnel accessing the MACG IT resources including the internet, or other resources authorised for official use. This includes any person working in a permanent, temporary, casual, contracted, voluntary or honorary capacity.

2. Policy

2.1. ACCEPTABLE USE

All individuals who access, use, or otherwise engage with MACG IT resources are required to:

a) respect the rights of all individuals, including other users;

b) only use MACG IT Resources for authorised purposes, and not in breach of relevant laws or contractual obligations;

c) not use MACG equipment, systems and infrastructure for non-commercial personal purposes beyond a reasonable amount, or to the detriment of MACG or its goals;

d) not access, distribute, store or display illegal, pirated or offensive material;

e) not use MACG equipment, systems or infrastructure for unauthorised personal financial or commercial gain;

f) not misrepresent the views of MACG, via use of MACG IT resources;

g) not conduct activities that consume excessive network bandwidth;

h) report suspected or actual security breaches to the Information Technology (IT) Service Desk in a timely manner; and

i) maintain the security and confidentiality of information generated or collected by MACG in accordance with the MACG Privacy Policy.

2.2. SECURE SYSTEM ACCESS AND USE

To protect access to MACG IT Resources, individuals are required to:

a) select strong passwords that are not easily discoverable;

b) securely store passwords that provide access to MACG systems or information;

c) only use the accounts provided by MACG for own individual use;

d) not share MACG-provided or self-selected passwords with other individuals not authorised by MACG;

e) keep personal and MACG-provided systems, used to access MACG information, free from known vulnerabilities by keeping up-to-date with authorised security updates;

f) maintain operational and up-to-date antivirus on personal and MACG-provided systems used to access MACG information;

g) not bypass or attempt to circumvent the MACG Security Controls or Protection Mechanisms;

h) not introduce malicious software such as viruses, worms, ransomware or trojans into the MACG environment; and

i) not use Hacking Tools (including sniffing, scanning, password guessing or exploitation) when accessing using or otherwise engaging with MACG IT Resources.

j) notify MACG of any device, account, or system compromise as soon as identified.

k) if using a personal device or non-MACG device to access MACG resources:

- Ensure that the device is always stored securely whilst accessing and/or storing MACG information
- Ensure that the device is password protected to the extent necessary to ensure that no third party can access MACG ICT resources or MACG information; and
- Immediately notify MACG of any breach of the Privacy Policy, and/or of any unauthorised access to MACG IT Resources or MACG confidential information (including resident information).
- Ensure that post-incident corrective actions are taken to immediately remediate information security compromise.
- Comply with all reasonable requests made by MACG and do all things reasonably required by MACG to ascertain the extent of any Privacy and/or security breach and to remedy the consequences of any such breach, including (without limitation):
    - providing MACG with such information as it requires to ascertain the extent to which the security/integrity of any device has been compromised and MACG confidential information (including resident information) has been disseminated to third parties; and
    - Within 24 hours of demand being made, providing MACG with evidence of corrective actions taken to address any security breach and/or exposure of device/systems and to remedy the same, and comply with consequences of the same.
- Ensure that the personal device otherwise complies with this policy at all times whilst accessing MACG IT Resources and/or storing any MACG information (including resident information).

- Destroy and/or permanently remove access to MACG IT Resources from all devices once it ceases being a provider/supplier to MACG, save to the extent required to comply with its contractual obligations to MACG, in which case the provision of this policy will continue to apply.
- Destroy and/or permanently remove any MACG confidential information from all devices once it ceases being a provider/supplier to MACG, information which is not of and incidental to the services provided by the Provider and not otherwise a record required to be preserved by law. Any MACG confidential information retained by the Provider on devices will continue to be dealt with in strictly compliance with the MACG IT Resources Policy and the confidentiality obligations contained within the Providers contract with MACG.
- Ensure that all external suppliers and partners, their staff, agents, and employees who access the MACG IT Resources are aware of and comply with this policy and if required by MACG, execute and deliver to MACG written acknowledgement that it, they, he or she has received a copy of this policy and is bound by its terms.

2.3. MONITORING AND COMPLIANCE

a) MACG monitors its information systems for compliance with this Policy. Breaches of this Policy constitute misuse of MACG information and information systems.

b) The Acceptable Use of IT Resources – 'Misuse' definition provides some examples of activities that constitute misuse of IT Resources. If misuse of IT Resources is detected or suspected, relevant disciplinary provisions will be invoked.

c) MACG may refer serious matters or repeated breaches to the General Manager ICT, General Manager Human Resources, or appropriate external authorities which may result in disciplinary and / or civil, and / or criminal proceedings.

d) MACG has a statutory obligation to report illegal activities and corrupt conduct to appropriate authorities and will cooperate fully with the relevant authorities.

e) To the extent allowed by law, MACG is not liable for loss, damage or consequential loss or damage arising directly or indirectly from the use or misuse of any Information Technology Resources.

3. Definitions

The following definitions apply for the purpose of this Policy:

1. Authorised Purposes means activities associated with work at MACG, or provision of services to or by MACG, which are approved or authorised by the relevant officer or employee of MACG in accordance with MACG policies and procedures or pursuant to applicable contractual obligations, limited personal use, or any other purpose authorised by the relevant officer or employee.
2. Hacking Tools means tools that are designed to facilitate the identification and exploitation of software or system weaknesses for the purposes of unauthorised access.
3. Information Technology Resources, or IT Resources, includes, but is not limited to:
    a) All computers and all associated data networks and systems, internet access and network bandwidth, email, hardware, data storage, computer accounts, all systems, media, software (both proprietary and those developed by MACG) and telephony services.
    b) Information Technology services provided by third parties that have been engaged by MACG.
    c) Information Technology services provided jointly, or as part of a joint venture between MACG and a subsidiary organisation owned by MACG or any other partner organisation.
4. Security Controls or Protection Mechanisms means systems or facilities implemented to restrict access only to individuals who are authorised to access or utilise the resource or information.
5. 'Misuse' includes, but is not limited to:
    a) use for any purpose other than an authorised purpose;

b) use that causes or contributes to a breach of any provision of a law, statute, regulation, subordinate instrument or code of practice or conduct applying to MACG or to which users are subject;

c) use that contravenes a MACG statute, regulation, rule, policy, procedure, or Cornerstones;

d) creating, transmitting, storing, downloading or possessing illegal material;

e) accessing, displaying, copying, downloading, distributing, storing or sharing pirated software, games, video, music, images, fonts, or other copyright material;

f) the deliberate or reckless creation, transmission, storage, downloading, or display of any offensive or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the appropriate use of Information Technology Resources for MACG work purposes;

g) use which constitutes an infringement of any intellectual property rights, or copyright of another person or organisation;

h) communications which would be actionable under the law of defamation;

i) communications which misrepresent a personal view as the view of MACG;

j) use which constitutes unauthorised recording, publishing, or communication of MACG communications, meetings, or conversations;

k) deliberate or reckless undertaking of activities resulting in any of the following:

- the imposition of an unreasonable burden on MACG Information Technology Resources;
- corruption of or disruption to data on MACG Information Technology Resources, or to the data of another person or organisation;
- disruption to other Authorised Users; or
- introduction or transmission of any hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs in any form including hyperlinks, executable code, scripts, active content, and other software into MACG Information Technology Resources.

l) circumventing authentication or access control measures, security or restrictions upon the use of any Information Technology Resources or account, including the unauthorised distribution or use of tools for compromising security, including but not limited to password guessing programs, cracking tools, packet sniffers or network probing tools;

m) betting online or gambling, other than participation in approved competitions where the primary purpose is social rather than financial;

n) accessing pornography;

o) use of any Information Technology Resources for sending junk mail or unsolicited bulk messages without MACG approval, for-profit messages, or chain, hoax or scam letters or messages;

p) use of any Information Technology Resources for the purposes of any private business whether for profit or not, or for any business purpose other than MACG business, without prior approval from authorised personnel;

q) subscribing to list servers, mailing lists and other like services for purposes other than MACG work or study or limited personal use;

r) participation in online conferences, chat rooms, discussion groups or other like services for purposes other than MACG work or study or limited personal use;

s) unauthorised accessing of information, including but not limited to unauthorised access to servers, hard drives, email accounts or files;

t) unauthorised reserving of, or exclusion of others from using, any Information Technology Resources;

u) breaching MACG Privacy Policy;

v) performing an act which will interfere with the normal operation of any Information Technology Resources;

w) unauthorised use of MACG logo;

x) representing that a message or material comes from another person without that person's authorisation;

y) knowingly running, installing or distributing on any Information Technology Resources a program intended to damage or to place excessive load on any Information Technology Resources, including without limitation programs in the nature of computer viruses, Trojan horses and worms;

z) failure to comply with the conditions of use imposed by an external provider when that provider's equipment or services are used in conjunction with any Information Technology Resources;

aa) providing a password or other means of authentication for any Information Technology Resources to another person without prior written approval from authorised MACG personnel, or failing to take reasonable care to protect a password or other means of authentication for any Information Technology Resources from being accessed or used by another person;

bb) failing to exercise reasonable care in the use, management and maintenance of Information Technology Resources, including but not limited to taking reasonable steps to ensure security and integrity of Information Technology Resources, including protection of equipment, systems and data from theft, unauthorised use or viruses;

cc) failing to comply with any reasonable instruction given by or with the authority of MACG authorised personnel to remove or disable access to material;

dd) using computing processing resources owned or operated by MACG or computer resources powered by electricity provided by MACG to perform mining of cryptocurrencies or brute forcing of cryptographic hash values for personal gain;

ee) aiding, abetting, counselling or procuring a person to do any of the things referred to above;

ff) inducing or attempting to induce a person to do any of the things referred to above;

gg) being in any way, directly or indirectly, knowingly concerned in, or a party to, any of the things referred to above;

hh) conspiring with others to do any of the things referred to above;

ii) attempting to do any of the things referred to above.

4. Related Documents

- Privacy Act, 1988
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Australian Privacy Principles (APP)
- MACG Privacy Policy
- MACG Information Security Policy which includes guidelines for Mobile Device Security