MAHI MIHINARE
ANGLICAN ACTION

COMPUTER AND INTERNET USE POLICY

Category:	Practice
Last Review Date:	July 2023
Next Review Date:	July 2026
Endorsed by:	The Anglican Action Missioner
Approved by:	The Anglican Action Mission Trust Board

Purpose

The purpose of this Computer and Internet Use Policy is to:

1. establish guidelines for the appropriate and responsible use of computer systems and the internet within the mission;
2. deter, prevent, and mitigate harm caused to the mission and its agents by digital communications;
3. ensure that the computers and internet connected devices in the agency are used only for professional purposes, and that no inappropriate material is viewed or downloaded.

Statement

Mahi Mihinare Anglican Action is committed to protecting the mission and its staff members from harm as a result of internet use.

Scope

This policy applies to all Anglican Action staff members as outlined in the Definitions section of this policy, and to Tangata Whaiora when using Agency computers under staff supervision.

Definitions

Employer	Employer means 'The Anglican Action Mission Trust Board', referred to as 'Mahi Mihinare Anglican Action' or 'The Mission' in this policy.
Agency	Agency means the Employer or Staff member as applicable.
Computer	'Computer' and 'internet connected device' refers to and include all Anglican Action computers and non-Anglican Action computers that are connected to the Anglican Action network and/or internet, all Anglican Action cell phones and non-Anglican Action cell phones that are connected to the Anglican Action network and/or internet and all other media and storage devices that are either Anglican Action property or connected to the Anglican Action network and/or internet.
Tangata Whaiora	Tangata Whaiora refers to any individual whom the mission agrees to provide a service or to whom the mission is legally obligated to provide a service.
User	Refers to anyone who accesses Mahi Mihinare Anglican Action systems and business-related applications which includes employees of Anglican Action, volunteers, students and third party users such as contractors and auditors.
Staff member	Staff member means all employees (permanent, fixed-term, or casual), consultants, contractors, service providers, students, and volunteers engaged by the Mission.

Policy

1. Acceptable Use

(a) All users must use computer systems and the internet in a responsible, ethical, and legal manner.
(b) Users shall not engage in activities that may disrupt or compromise the security, availability, or integrity of computer systems or network resources.
(c) Users must respect intellectual property rights, including copyrights, trademarks, and patents, and should not download, copy, or distribute copyrighted material without proper authorization.
(d) Users must not use computer systems or the internet for personal financial gain, commercial activities unrelated to their work, or any illegal activities.
(e) Users should exercise caution when sharing personal information online and should not disclose sensitive information about the organization or its tangata whaiora without proper authorization.

2. Prohibited Activities

(a) Users are strictly prohibited from accessing, transmitting, or storing material that is obscene, offensive, defamatory, or discriminatory, as per New Zealand's Harmful Digital Communications Act 2015.
(b) Users shall not engage in any form of cyberbullying, harassment, or unauthorized monitoring of others' computer activities.
(c) Users must not engage in any form of unauthorized hacking, unauthorized access to systems, or any activities that could compromise the security of computer systems or networks.
(d) Users shall not use computer systems or the internet for any illegal activities, including but not limited to distributing malware, engaging in fraud, or participating in illegal file-sharing activities.
(e) Users should never download or install any commercial software, shareware, or freeware onto network drives or disks for any reason.
(f) Users should not download or open any email attachments from unknown sources and must immediately inform Anglican Action management if unsure.

3. Information Security

(a) Users must protect their login credentials and should not share them with unauthorized individuals.
(b) Users must not attempt to gain unauthorized access to other users' accounts, computer systems, or networks.
(c) Passwords must be created and managed in accordance with the following:
    i) New passwords cannot be the same as the previous four passwords.
    ii) Passwords must be at least nine (9) characters in length
    iii) Passwords must contain at least one number
    iv) Passwords should not be shared, and treated as sensitive, confidential information.

Key Accountabilities & Responsibilities

Person / Party	Responsibilities
Governance	Review policy every two years or as required
Management	Ensure that staff members are aware of this policy and processes
Leadership	Ensure that staff members are aware of this policy and processes
Staff	Have access to this policy and understand their obligations under it

Related Policies, Legislation, Regulations and Documents

- Privacy Act 2020

- Harmful Digital Communications Act 2015
- Copyright Act 1994
- Crimes Act 1961
- Anglican Action Code of Conduct
- Privacy and Personal Information Policy
- Storage of Information Policy
- Social Media Policy