Acceptable Use of Technology Policy

Drafted By	Jessica Macpherson	Reviewed By	Matthew Craven, HWL Ebsworth
Version	2	Approved By	Board
Category	Operational Management	Approved Date	18 November 2020
Type	Information Technology	Review Date	18 November 2022

Purpose

This policy outlines the requirements for acceptable use of the computer network, including internet and email.

Scope

This policy applies to all personnel of the organisation.

Definitions

The organisation, St Kilda Mums, we, us, our – St Kilda Mums Inc., also trading as Eureka Mums and Geelong Mums

IT Facilities – any and all computers, tablets, telephones, computer networks, internet access services, email services, software, hardware and other information technology facilities owned, controlled or provided by the organisation for use by users.

Personnel – staff and volunteers of the organisation, whether paid or not.

User – means a member of Personnel or any other person whom the organisation allows to use any of its IT Facilities from time to time.

Policy

The primary purpose for which access to the internet and email is provided to personnel is to assist them in carrying out the duties of their employment.

Personnel may use the IT facilities provided by the organisation for:

- Any work and work-related purposes;
- Limited personal use (for details see Procedures, below);
- More extended personal use under specific circumstances (for details see Procedures, below).

Other users may be authorized by the organisation, subject to compliance with this policy. The organisation must specify the permitted purposes for use of the IT Facilities in each case.

1. Responsibilities

It is the responsibility of the CEO to ensure that:

- Users are aware of this policy;

- any breaches of this policy coming to the attention of management are dealt with appropriately.

It is the responsibility of all users:

- to ensure that their usage of IT Facilities conforms to this policy;
- not to use the IT Facilities to disclose, transfer or use confidential information other than for legitimate purposes permitted by the organisation;
- to keep passwords and other security credentials secret, and to notify the IT Manager immediately if they suspect another person may have discovered them;
- to notify the IT Manager immediately if they suspect there has been any unauthorised or unacceptable use of IT Facilities;
- to notify the IT Manager immediately if they believe the IT Facilities may be impacted by errors, viruses, malicious code, or other unusual behaviour.

2. Use of IT facilities

2.1. Limited personal use

Limited personal use of the organisation's IT Facilities is permitted where it:

- Is infrequent and brief;
- Does not interfere with the duties of any Personnel;
- Does not interfere with the operation of the organisation;
- Does not compromise the security of the organisation's IT Facilities;
- Does not impact on the organisation's electronic storage capacity;
- Does not decrease network performance (e.g. large email attachments can decrease system performance and potentially cause system outages);
- Incurs no additional expense for the organisation;
- Does not violates any laws or infringe the rights of third parties (including intellectual property rights);
- Does not compromise the confidentiality requirements of the organisation;
- Does not fall under any of the 'unacceptable use' clauses outlined below.

2.2. Permitted extended personal use

It is recognized that there may be times when Personnel need to use the internet or email for extended personal use. An example of this could be when a member of Personnel needs to use the internet to access a considerable amount of materials related to study they are undertaking. In these situations, it is expected that:

- The member of Personnel advises and negotiates this use with their manager first;
- The time spent on such personal use replaces all or part of the person's break/s for that day, or that they adjust their timesheet accordingly for that day.

It is not expected that personnel need to advise or negotiate with their manager for personal use that would be reasonably considered to be of a limited nature.

2.3. Unacceptable use

Personnel must not use IT Facilities (including internal email access) provided by the organisation to:

- Create or exchange messages that are offensive, harassing, defamatory, obscene or threatening, or which infringe any third-party rights or any law;
- Visit websites containing objectionable (including pornographic) or criminal material;
- Exchange any confidential or sensitive information held by the organisation (unless in the authorised course of their duties);
- Create, store or exchange information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies);
- Use internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities;
- Create or exchange advertisements, solicitations, chain letters and other unsolicited or bulk email.

3. Monitoring

Personnel must be aware that use of IT facilities, and any communications made using IT facilities, is not private.

By using the IT facilities, the user consents to the organisation monitoring and reviewing all use of the IT facilities. The organisation may conduct electronic surveillance at any time.

This may include:

- monitoring and reviewing use of the IT Facilities;
- reading email messages sent, received or stored on the organisation's email services or devices owned by the organisation;
- reviewing and logging internet activity by users, including websites visited, and information uploaded and downloaded utilising any IT Facilities; and
- by utilising GPS and related functionality, checking the location of any IT Facility devices owned by the organisation (e.g. a laptop or mobile phone) that are in the possession of a user.

The organisation may block any communications (e.g. emails) which are to be delivered to or via any IT Facilities where permitted by law to do so, including where it suspects that such communication infringes this policy.

Users should be aware that surveillance records may be:

- reviewed and audited by the organisation (including by senior management, the IT Manager and any user's manager) at any time, whether intermittently or regularly;
- stored by the organisation;
- transmitted by the organisation to a third party;
- used in the course of an investigation;
- used by the organisation and disclosed to third parties for the purposes of enforcing this policy and any of its other policies;
- used by the organisation in legal proceedings; and
- otherwise dealt with by the organisation in any lawful way.

Personnel may consult with the organisation if they have any queries regarding the nature and extent of the IT surveillance.

Review

This policy will be reviewed and updated every two years or sooner if required. It will be approved by the Board and readily accessible by all staff via the People & Policy App on Salesforce.

This policy will be published on the organisation's website.

Any questions in relation to the policy, please contact the CEO.

Reference Documents

a. Occupational Health & Safety Policy

b. Social Media Policy

c. Code of Conduct