Acceptable use (internet and technology)

"I trust the organisation and its staff."

Intent

We have access to and use a variety of communications and networking resources including email, texting and internet. These resources must be used responsibly and in accordance with our Code of Conduct.

Responsibilities

Management will:

- ensure our operational systems are secure
- ensure technology is adequately maintained and updated for organisational purposes
- ensure team members understand they must comply with this and other policies when using technology
- monitor access and use of our technology.

Team members will comply with this policy.

Requirements

User accounts assigned to each staff member for access to organisational files must be mainly used for organisational purposes.

Kaimahi are responsible for activities using their accounts. They must not share their user name and/or password with anyone else or allow others to use their account.

A level of personal use is allowed, provided it does not detract from our mahi or interfere with others' work.

Any software or files downloaded through the internet into the organisation's resources are owned by the organisation and must only be used in accordance with their licence or copyright.

Internet and email access must not be used to download and install software games or utilities (except commonly used files such as Word documents, PDFs).

On-line conferences, discussion groups, email lists and other like services must be relevant and used for work purposes or related to professional development activities.

Kaimahi must exercise extreme caution when opening email attachments received from unknown senders, which may contain malware.

The Communications principles of the Harmful Digital Communications Act 2015 must be complied with.

Prohibited activities

Unauthorised access and use of another person's account details either with or without their knowledge is prohibited.

User accounts and organisational equipment must not be used to:

- gamble
- receive or make communications, edit, record or otherwise deal with material that is obscene, objectionable or likely to offend
- transmit sensitive business-related information about the organisation unless authorised to do so
- transmit personal information about a client or colleague except in accordance with the Protection of privacy policy
- solicit for personal gain or profit
- access another person's electronic files, email or other electronic communications (unauthorised)
- try and circumvent the user authentication or security of any host, network or account.

- issue or reply to "mailbombs"(ie when a large volume of email sent to a single or many addresses with malicious intent)
- upload or download commercial software in violation of copyright laws
- download any software or electronic files without reasonable virus protection measures in place
- express personal views as the organisation's views
- forge user authentication or security. This includes, adding or attempting to add user's addresses to any internet mailing list, altering header information to conceal own email address.
- any activity that violates the law, our policies and/or Code of Conduct
- extensive private use that interferes with work productivity and/or costs our organisation an unacceptable amount of money.

Any violation of this policy will be dealt with as a disciplinary matter and may result in revoking or restricting the right to access/use electronic communications.

Mobile phones

The organisation's cell phones must be responsibly and carefully used. Wifi should be used when possible.

Limited personal use of phones while at work is permitted, provided it does not interfere with operations or impact adversely on service delivery and colleagues.

Phones must be charged and turned on for all travelling to/from and during visits with rangatahi(the phone can be on silent).

Organisational mobiles must only be used by the kaimahi authorised to use it.

If the mobile phone is a personal phone with organisational software on it, use by others (such as tamariki) must be monitored to ensure they do not access the software applications.

Helpful links

Remote working information safeguards

Disciplinary action

Misconduct

Social media

Harmful Digital Communications Act 2015

Review

Date: January 2021

Next review: by December 2023