ICT Acceptable Use Policy

Policy owner: Group General Manager Strategy, Capability and Performance
Policy reviewed by: The Board on the recommendation of the Audit and Risk Committee
Policy approved by: The Board on 10 April 2025
Next review due: 30 April 2028, with any amendments to be considered by the Audit and Risk Committee and approved by the Board for implementation.
Distribution: Available online in Ipu.

This policy is provided to all staff and Board members. It is the responsibility of each staff and Board member to understand and apply this policy. It also applies to contractors engaged by Education New Zealand (ENZ). It is the responsibility of the Manager engaging the contractor to ensure they are aware of all ENZ policies while working for ENZ.

Purpose

This Policy informs and guides Education New Zealand (ENZ) staff to use ENZ technology in a safe, secure and productive manner. It supports ENZ in meeting its statutory obligations, in particular the Privacy Act, Official Information Act, Copyright Act and Public Records Act obligations.

Scope

This policy applies in New Zealand and overseas. It applies to any ENZ employee, intern, contractor or consultant (including but not limited to any 3rd parties and their suppliers/agents and ENZ Board Members and those working under contract for services) working with ENZ devices or connecting to ENZ ICT systems or ENZ ICT related services.
Except where local legislative requirements conflict with this policy, it should be followed in offshore locations. For offshore staff, local legislation takes precedence over this policy.

Hardware and software authorised for use

1. User may use either a computer issued by ENZ (ENZ supplied device) or a personal computer (non-ENZ supplied device) to access ENZ systems.

2. Where a device has been issued to an individual by ENZ (ENZ supplied device), only approved software may be installed and used on that device. This restriction includes all free or open-source software.

3. If you are using a non-ENZ supplied device, you must have a software-based firewall and anti-virus software installed on that device.

Limit your personal use

Limited personal use of ENZ ICT resources is acceptable provided it does not:

1. Unduly impact your work-related productivity;

2. Threaten the security of ENZ's ICT environment, or utilise significant network bandwidth or storage capacity (e.g. non-business-related downloading, streaming or storage of music, gaming, video or image files);

3. Breach copyright, breach New Zealand or international law, or otherwise bring ENZ into disrepute.

ENZ will not accept any direct or indirect liability for any damage or loss resulting from personal use of its ICT environment.

Manage your user accounts and passwords appropriately

1. User accounts are assigned on an individual basis and must not be shared.

2. Users are responsible for all actions performed under their user accounts. This responsibility cannot be delegated.

3. Ensure that the passwords you choose are difficult for others to guess and are not recorded where others may learn what they are.

4. Passwords must not be shared. If password security is breached, the password should be changed immediately and the ICT team advised.

5. Managers are permitted to delegate their access within applications to an Assistant using built-in delegation features.

6. The sharing of passwords for internal ENZ systems is prohibited unless there are exceptional circumstances and it has been agreed in advance with the Director ICT and Property.

7. The only circumstances where the sharing of passwords is permitted is for external systems where there is a generic login for access eg SurveyMonkey

Keep our systems and information secure

Users must not:

1. Install unauthorised software applications on ENZ supplied devices;

2. Perform actions or use tools that are designed to circumvent security controls imposed by the ENZ ICT systems;

3. Connect unauthorised peripheral hardware devices to ENZ supplied devices;

4. If in doubt as to what devices and software are approved for use with ENZ supplied devices, contact the IT Team.

ENZ is required by law to protect all information held in its care. All users are individually responsible, through employment agreements, independent contractor agreements, and supplier agreements, for the secure creation, use and disposal of such information.

Respect intellectual property

Users must not knowingly violate the rights of a person or company protected by copyright, trade secret, patent or other intellectual property right, or similar laws or regulations. This includes downloading, or distribution of copyrighted music, videos, photographs from magazines, books and the installation of any copyrighted software for which ENZ does not have an active license.

Secure your portable devices

1. Any information taken from ENZ premises must be kept safe and treated with utmost care, irrespective of its form (paper or electronic) or the media on which it is stored.

2. Portable devices such as (but not limited to) laptops, tablets, smartphones, portable hard drives and memory sticks must not be left unattended when taken outside of ENZ's physical premises or other secure locations (e.g. your home environment)

Using messaging appropriately

All information sent or received by ENZ is subject to the Official information Act and may be required as part of a request by external parties

1. Business-related email sent from, or received to, ENZ email accounts must be kept and managed in line with the Information Management policy (see the ENZ SharePoint system or Ipu for the latest version.)

2. Users can be held to account for content sent via email, text, instant message, social media/blogs etc. that has the potential to bring ENZ into disrepute.

3. Users should not send messages from another person's account without the appropriate delegation.

4. Users should not:
    a. Send a reply to a message containing ENZ information without confirming the identity of the original message's sender;
    b. Auto-forward emails from ENZ email accounts to external addresses;
    c. Publish work email addresses on publicly accessible websites unless there is a good reason to do so;
    d. Forward unknown or suspicious email attachments;
    e. Click on links or attachments in suspicious emails;
    f. Propagate or initiate chain letters.
    g. Send official ENZ communications from a personal email address.
5. Emails that contain security classified information (i.e. RESTRICTED and above) must be secured using approved procedures and products. Emails sent to other Government agencies currently use SEEMAIL if the receiving agency has a SEEMAIL system. This gateway operates automatically.
6. Information classified above RESTRICTED must not be stored, transmitted or processed on the ENZ ICT environment.
7. ENZ reserves the right to inspect all emails held on ENZ systems and may block some incoming and outgoing messages.

Don't access, store or send incorrect or inappropriate material

1. ENZ technology must not be used in any way that may impact adversely on its reputation, or on the performance of its ICT systems.
2. It is expressly prohibited to use ENZ systems or technology to undertake activities that are illegal under New Zealand or relevant international laws.
3. The use of ENZ technology for the following (or similar) purposes is expressly prohibited (unless explicitly approved for work purposes):
    a. Accessing, distributing or storing offensive, illegal, sexually explicit, pornographic, obscene or otherwise inappropriate material;
    b. Accessing or promoting on-line wagering, betting or gambling sites;
    c. Accessing, sending, distributing or storing material that constitutes defamation, harassment (of any kind), interference, hatred, or discrimination based on age, race, disability, religion, gender, sexual preference or any other unlawful grounds.

Maintain confidentiality

Users must not:

1. Disclose sensitive information to anyone who is not authorised to receive it, or who does not “need to know” it for business purposes;
2. Send or distribute personal information that breaches an individual’s rights under the Privacy Act;
3. Communicate, or provide unauthorised access to information about, or lists of, ENZ employees or customers to parties outside of ENZ or its vendors and third-party contractors.

Avoid reputational risks

To avoid damaging ENZ’s reputation, users must not:

1. Make any misrepresentation about ENZ or its affairs;
2. Publish or update information on web sites (including blogs and social networking sites) that may lead to personal views being published under ENZ identification – including the use of ENZ email addresses for personal postings;
3. Send or distribute material that involves political lobbying.

Act ethically

Users should not:

1. Misrepresent their identity, including the origination address of an email;
2. Distribute or store unauthorised material in support of, or for the operation of, any commercial business other than that of ENZ;
3. Store an amount of personal material on ENZ systems that would have unreasonable and inappropriate effect on the productivity or cost of those systems;
4. Conduct any illegal or unethical activity.

Restricting and monitoring user ICT activity

Internet content is monitored and any site or content that puts ENZ at risk or is inappropriate may be blocked or limited.

ENZ monitors the use of all ENZ ICT (logins, data, email, phone calls, text messages, instant messages, files and cached files) and may use that information should operational needs require it.

Access to ENZ technology and services such as email, telephony and the Internet is recorded in log files and monitored. Information may detail web sites visited, files downloaded, time spent on the Internet, and related information. Use of monitored log files may be deemed necessary:

1. At the direction of a legislative or regulatory body;
2. Pursuant to an application for discovery in legal proceedings;
3. If ENZ reasonably suspects there has been a breach of this policy, its Code of Conduct, another policy or procedure, the law, or external regulation, such as a Government standard;
4. As part of standard or routine system maintenance or optimisation;
5. As a periodic review of compliance with ENZ policies;
6. As part of management reporting.

Mobile device use

Your mobile device (such as, but not limited to, iPhones) is provided for work purposes. If ENZ deem use is excessive or irresponsible, we may take steps to recoup costs. Reasonable personal use is permitted but should be restricted to local or national calls, text messages and limited internet access. You may not use any of the functions of your mobile device, including camera functions for:

1. illegal or illegitimate purposes
2. any activities that may cause ENZ embarrassment or bring it into disrepute
3. viewing, accessing, or creating offensive or pornographic materials

When travelling:

1. Users should not use data roaming except in countries whereby we have data roaming agreements (see the Senior ICT & Properties Specialist for the current list of supported countries).

2. If you are travelling and need to speak to a colleague, text them and ask them to call you as this is likely to be a much cheaper option than you calling them from your mobile

3. If you are travelling with a colleague who is on a local plan and they have a mobile device, use theirs for calling as it is typically cheaper

4. If you're based in a hotel and they have reasonable rates, utilise the hotel phone.

5. If you have free or cheap internet access, use the Teams or Zoom apps for video or voice calling.

Health and safety

To ensure safe use of ICT equipment and facilities when this is required as part of your job, you need to:

1. read all material provided by ENZ on the safe use of devices

2. contact the People & Capability team or your manager if you need further advice on the safe use of equipment

3. follow the advice provided from any workstation assessment provided at your work site

4. ensure you do not engage in any illegal activities (for example, using a mobile phone while driving).

Cybersecurity Training

Annual Cybersecurity Training:

All employees are expected to complete the annual Cybersecurity Training each year. Existing employees are to fulfil this requirement no later than the end of March each year. New employees are to complete the training within one month of commencing employment with ENZ.

Security Score Maintenance:

All employees are expected to maintain a Security score of 630 or more.

All users must achieve and maintain a rating of 'Good' in the organisations Cyber Security Training tool. This rating must be achieved within one month of commencing work at ENZ and within one month of resuming work at the start of a new calendar year when the annual Cyber Security training exercise becomes available.

Breaches of this policy and consequences

A breach of this policy may expose ENZ to a wide range of risks. It is each user's responsibility to understand how this policy applies and the implications of its breach:

1. For employees – performance management or disciplinary action which could involve the termination of employment

2. For contractors, employees or agents of a supplier of services to ENZ – termination of the engagement, the request for the user's removal from ENZ or termination of the supplier agreement.

Definition of terms

For the purposes of this policy, "technology" refers to the electronic Information and Communication Technology (ICT) systems and devices that are used, operated or accessed by ENZ including:

1. Hardware (includes but is not limited to: computers, laptops, removable media devices, telephone systems, cabling, support devices, printers); and

2. Software and systems (includes but is not limited to: the Internet, intranet, and associated content, software applications or tools, databases, email and other electronic messaging systems).

Where this policy refers to "sensitive" information or data, in lower-case letters, it indicates the information requires some special attention to manage its distribution and access. The words "must" and "should" are used in this policy as defined in section 1.1 of the New Zealand Information Security Manual (current version is December 2020 v3.4)

Relevant Legislation

1. Privacy Act 2020

2. Official Information Act 1982

3. Copyright Act 1994

4. Public Records Act 2005

Other related documents

1. ENZ Code of Conduct
2. New Zealand Information Security Manual (NZISM)
3. Guidelines for using Generative Artificial Intelligence (GenAI) at ENZ

Measures

The impact of this policy will be evaluated by measuring:

1. ICT misuse incidents, complaints
2. Recorded breaches of this policy
3. Automated usage monitoring

Help

For clarification about the application of this policy in a particular situation, contact:

1. Your team leader or the equivalent if you are a contractor, or an employee or agent of a supplier of services to ENZ;
2. Director – ICT and Property
3. Senior ICT & Properties Specialist