NZALS
New Zealand Artificial Limb Service
Peke Waihanga, Aotearoa

Internet and Email Use Policy

Table of Contents

1 Background

1.1 The internet and email facilities are recognised as valuable tools to help NZALS maintain an IT environment which efficiently supports core business and simplifies ease of access to information. However, the use of email and the internet carries some risk to employees, others, and NZALS.

2 Purpose

2.1 This Policy sets out employees and NZALS' responsibilities and obligations in relation to electronic communication and the use of email and the internet. This Policy emphasises that any use of the internet and/or email should reflect the same standards of professional conduct and ethics that are expected and maintained by employees in other areas of their work.

3 Scope

3.1 This policy applies to all NZALS employees and Board members, and to any other person(s) authorised to have access to the NZALS' information systems.

4 Policy

4.1 The personal declaration attached to this Policy must be signed before access to NZALS information systems is granted.

4.2 This Policy is formed on the basis of the following principles:

(a) NZALS and employees' obligations under the Privacy Act, Health Information Privacy Code, Official Information Act, and Public Records Act apply to all information held by NZALS, whether in physical or electronic form, and including records held in NZALS business systems and email accounts;

(b) Email and other electronic data must be used primarily for business purposes, and in a manner which does not risk damaging NZALS' reputation and contributes to the safe, effective and accountable operation of NZALS business;

(c) Responsibility when using the internet and/or email lies with the individual employee. It is the individual employee who is accountable for any activity that does not comply with this Policy. This includes, but is not limited to any statement or use that breaches the law.

4.3 All material stored on electronic devices operated by NZALS, or on NZALS' behalf, is the property of NZALS. This includes material stored on desktop computers or portable devices supplied by NZALS, and material which may have been created for personal use, but has been stored on a NZALS system and/or device.

4.4 This Policy will be reviewed regularly to take into account the changing nature of email, internet and IT as well as the law surrounding its use. All sections in this Policy will be subject to additions and amendments by NZALS at any time.

5 Definitions

5.1 **Employee** – For the purposes of this Policy, 'employee' includes employees, Board members and external contractors or any person authorised to use NZALS electronic systems.

5.2 **Offensive material** – Includes messages or pictures that are obscene, insulting, harassing, sexist, pornographic, threatening, illegal or otherwise inappropriate. This includes but is not limited to messages or pictures that would come within the definition of 'offensive material' in the Films, Videos and Publication Classification Act, sexual or racial harassment under the Human Rights or Employment Relations Acts, or material or messages could serious emotional distress under the Harmful Digital Communications Act.

6 Acceptable email and internet use

6.1 NZALS recognises the value of the internet and email as important tools for NZALS in managing its business. However internet and email use can pose significant risk to NZALS and individual employees. When using the internet and/or email employees should be cautious and exercise the same common sense and good judgement they use elsewhere. Employees must not use the internet, social media, or email in such a way as to interfere with the duties of their employment (or another's) or that is likely to expose NZALS to significant cost or risk of liability. Individual employees and NZALS may be exposed to legal action, including prosecution under the Films, Videos and Publication Classification Act, the Harmful Digital Communications Act, and human rights and health and safety legislation, for offensive or otherwise inappropriate material that is emailed or sent via any other electronic means at work or from a device operated by NZALS.

Email use

6.2 All email messages sent with the NZALS email address in the 'From:' or 'Reply To:' header, must be accompanied by the approved disclaimer to the effect that the views of the sender may not represent those of the NZALS. This disclaimer is provided in the template signature found in the Creating an Email Signature Procedure.

6.3 When sending an email to several people, a group should be set up in the email system and used. This prevents disclosure of personal email addresses and means that the members of the group will be protected from any virus that penetrates the security system and is aimed at addressees.

6.4 An email from a NZALS device is effectively communication on behalf of NZALS and may end up having a much wider distribution than intended. Communications by email must be courteous and professional. Employees should not say something in an email that they would not be comfortable putting in a letter or memorandum. It is inappropriate to send heated messages or exchanges by email. NZALS is subject to the Official Information Act therefore all emails received and sent may be required to be disclosed.

Reducing the risk of data leakage when using email

6.5 Email breaches of privacy represent a significant risk to NZALS, NZALS stakeholders, patients and employees. To minimise the risk of an email accidentally being sent to the wrong person, employees should always check the addressee carefully before sending an email.

6.6 When sending information internally and the information to be shared:

(a) Contains bulk data; or

(b) Allows someone to easily identify a patient or employee; or

(c) Contains information that could breach someone's privacy;

then the information should not be attached or included in the body of the email. The recipient(s) should instead be sent a hyperlink to the desired file which has been moved to the 'Temp File' on the National Drive. Information on hyperlinking and using the temp file can be found here.

6.7 To limit the possibility of a privacy breach when sending information by email to an external recipient, the following rules should be applied:

(a) Only one patient is to be referenced in an email (unless the exception 8.7e of Data Protection Policy for regional clinic information applies); and

(b) When attaching a document(s), the document(s) should be opened and double checked to ensure it contains the intended information only; and

(c) The employee should double check that the correct recipient(s) and correct email address(es) is/are selected before sending the email.

Internet use

6.8 The use of the internet is provided to employees as part of the standard IT desktop access. Access must only be provided once the employee has signed the personal declaration attached to this Policy. Access to the internet may be revoked by NZALS at any time at its sole discretion.

6.9 Employees are responsible for ensuring their password is kept safe and confidential and for ensuring other persons do not make use of their access.

6.10 Web browsing is provided primarily for NZALS business use and associated research and educational activities.

Personal use of emails and the internet

6.11 Email and internet access is primarily provided for business use. Reasonable use of the Internet and email is allowed for private purposes.

Personal use of emails

6.12 Personal emails/non business emails may be sent and received, provided that:

(a) They do not, where possible, have any electronic documents attached, especially when receiving emails. If a received email has an attachment, sensible judgement about it must be used. For example, if something is received and the employee is uncertain about its security/origin/safeness, they should consider whether it should be immediately deleted. If a personal correspondent continues to send an employee documents as attachments, or documents that the employee suspects are not acceptable, the employee must ask the person to stop, and should inform IT if this does not happen.

(b) They are not distributed internally; and

(c) They are not signed off with a NZALS electronic sign off attached.

6.13 Improper use of email may lead to loss of access to the system and/or disciplinary action in accordance with the Code of Conduct and NZALS Disciplinary Policy.

Personal Internet access and use

6.14 The internet may be accessed for reasonable personal purposes provided that the use in each case:

(a) Is moderate in time and does not incur cost for the organisation; and

(b) Is carried out at a time that does not interfere with the employee's employment duties or those of their colleagues (e.g. use it during lunch and tea breaks); and

(c) Does not contain items involving storage of pictures, music, etc.; and

(d) Is not, in any way, unlawful or in conflict with the values and vision of the NZALS.

6.15 NZALS expects employees to exercise good judgement and common sense when accessing the internet in NZALS time and/or on devices operated by NZALS.

7 Unacceptable email and internet use

Downloading additional software

7.1 All NZALS software and hardware has been specifically selected and configured to minimise exposure or attacks on the NZALS network from outsiders. Altering the configuration or installing any software must not be attempted. Downloading any further software is forbidden. Any downloads and/or configuration to an employee's system account is blocked by user permissions.

7.2 Employees are given permission to download and install some selected software (for example 'Google Chrome'). If an employee has a request to download any other software for work purposes they should approach their appropriate IT delegate.

Other non-acceptable uses

7.3 NZALS expects employees to use their judgement and common sense when using NZALS email or internet resources. Anything that contravenes New Zealand laws will amount to an unacceptable use. Except in the course of an employee's duties or with the express permission of a manager, internet and email provided by the NZALS may not be used for:

(a) Non-business purposes such as:

- unreasonable or excessive personal use during business hours which interferes with the duties of the employee or a colleague;
- generation, transmission, display or storage of potentially obscene material or offensive information. This includes, but is not limited to profanity, offensive jokes, material derogatory to any ethnic, gender-based or other groups of people, or sexually explicit material, or any other activity that is, or is likely to be, a breach of the Communication Principles set out in the Harmful Digital Communications Act, or comes within the definition of 'offensive material' in the Films, Videos, and Publications Classification Act. Such material may not be downloaded, archived, stored, distributed, edited, reproduced or recorded using the NZALS' network, printing or computing resources. If such a website is accidentally accessed, the manager must be informed, who will record the date and time of the accidental access;
- gambling of any sort;
- downloading of software (including messaging software), data or media files, other than by way of brief e-mail attachments or small amounts of data (e.g. personal bank statements) for personal use;
- storing of non-business related applications on the network or PC;
- promotion of an employee's own business or others business or private activities or personal commercial purposes;
- creating or sending 'spam', as defined in the Unsolicited Electronic Messages Act, including sending unsolicited bulk email and subscribing to mailing lists, and opening, replying to or forwarding chain letters.

(b) *Activity that directly affects NZALS. For example:*

- personal use that interferes with the availability, performance or maintenance of the NZALS' computer systems or networks;
- altering or deleting the NZALS' documents and records without authority;
- inappropriately handling or transmitting personal or health information or images;
- unauthorised attempts to use, access or damage any electronic device, system, or network;
- disseminating confidential information held by the NZALS (see Privacy Policy). This includes disseminating personal contact information of Board members, stakeholders, patients or employees of NZALS without their consent;
- passing off an employee's own views as representing those of NZALS.

(c) *Illegal activity, such as:*

- downloading or distribution of pirated software or data, or use of software/files downloaded from the internet in any way that is not consistent with licencing and/or copyright agreements;
- transmission of, or any other activity that involves, harassing, defamatory or threatening behaviour or messages that would contravene the Films, Videos, and Communications Act, Harmful Digital Communications Act, or that constitutes harassment or discrimination under the Human Rights Act, Employment Relations Act, or Harassment Act;
- using NZALS devices in violation of any applicable law or regulation, including, but not limited to, advertising, transmitting, or otherwise making available Ponzi schemes, pyramid schemes, fraudulently charging credit cards, pirating software, or making fraudulent offers to sell or buy products, items, or services;
- knowingly engaging in any activities that disrupts the use of or interfere with the ability of NZALS or others to effectively use NZALS system or any connected network, system, service, or equipment. This includes deliberate propagation of a virus, worm, Trojan horse, malware, pinging, flooding, flaming, mail bombing, trap-door, back-door or any other malicious program code, or denial of service attacks;
- infringing copyright, copying electronic files without permission or breaching the terms of any licence;
- accessing illegally or without authorisation computers, accounts, equipment or networks belonging to another party, or attempting to penetrate security measures of another system. This includes any activity that may be used as a precursor to an attempted system penetration, including, but not limited to port scans, stealth scans, or any other information gathering activity.

Using personal devices for work purposes

7.4 Refer to the Mobile Device Usage Policy.

8 Monitoring

8.1 The NZALS may monitor and trace any internet, social media, or email use occurring on NZALS equipment or accounts. This may include usage patterns, key strokes, and any other activity on NZALS' IT systems and email. NZALS may:

(a) Deny access to any website that is not essential for the execution of an employee's duties;

(b) Read any communication on NZALS' IT system;

(c) Act on any behaviour/action observed through monitoring or tracking. NZALS may access and/or disclose all information on its network and/or stored on its equipment including employees' computer and email without the employee's consent in order to ensure compliance with this Policy and the law.

8.2 NZALS reserves the right to automatically block or isolate email attachments or unsolicited emails or an employee's access to and use of emails or the internet from devices operated by NZALS.

9 Publication of information

9.1 For information on internet publications see the Communications Policy.

10 Consequences of unacceptable use

10.1 NZALS takes very seriously any inappropriate use of the internet, social media or emails. NZALS will review any alleged breach of this Policy on an individual basis. If the alleged breach is considered to be of a serious nature (whether an individual incident or a number of lesser breaches), such matters will be referred to the Chief Executive for further action. Any breach of this Policy is considered misconduct and could constitute serious misconduct under NZALS' Code of Conduct and Disciplinary Policy, and may lead to loss of access to NZALS' IT system, and/or may result in disciplinary action, including dismissal.

11 Specific responsibilities

Party	Responsibilities
All Employees	• Ensure they adhere to the boundaries and guidelines set out for internet and email usage in this Policy.
Managers	• Ensure every employee has read this Policy, and signed and returned the form attached, and that the signed form is retained in the employee's personnel file. • Ensure that all employees (including themselves) have a clear understanding of, and comply with, this Policy. • Ensure that all employees are informed of any updates to policy. • Monitor and appropriately manage any instances of unacceptable practice.
CEO	• Ensure this Policy is reviewed and updated in a timely manner as required.
The Board	• All Board members must comply with this Policy.

12 Legal compliance

- Crown Entities Act 2004
- Employment Relations Act 2004
- Films, Videos, and Publications Classification Act 1993
- Harmful Digital Communications Act 2015
- Harassment Act 1998
- Health Act 1956
- Health and Safety at Work Act 2015
- Health Information Privacy Code 1994
- Health (Retention of Information) Regulations 1996
- Human Rights Act 1993
- Official Information Act 1982
- Privacy Act 1993
- Protected Disclosures Act 2000
- Public Records Act 2005
- Unsolicited Electronic Messages Act 2007

13 Related Policies, Procedures and Forms

- Discipline Policy
- Code of Conduct Policy
- Communications Policy
- Data Protection Policy
- *Records Management Policy*
- Privacy Policy
- Mobile Device Use Policy
- Creating an Email Signature Procedure
- Hyperlinking Guidelines

14 Revision History

Author	Version number	Version date	Description of changes
CEO	3.2	February 2016	Email exception for regional clinic
CEO	3.1	December 2015	Incorporated Claro Law feedback and updated brand
Compliance Advisor	2.3	June 2015	Addition of an personal copy of the acknowledgment page
External Contractor	2.2	May 2014	Adopted MM and GAF Edits.
External Contractor	2.1	February 2014	Added FM and AG amendments.
External Contractor	1.2	February 2014	Reformatted Policy and amendments
Executive Manager Corporate	1.0	September 2002	Original policy

NZALS
New Zealand Artificial Limb Service
Peke Waihanga, Aotearoa

Declaration: Acceptable Internet & Email Use (Personal copy)

Please retain this copy to confirm you have read and understood the NZALS Acceptable **Internet and Email Use** Policy.

I have read and understood the NZALS Policy on Acceptable Internet and Email Use, and agree to abide by this Policy.

_____

Name

_____ _____

Signed Date

PAGE HOLDER ONLY

Please return page 13 to your Manager including signature

NZALS
New Zealand Artificial Limb Service
Peke Waihanga, Aotearoa

Declaration: Acceptable Internet & Email Use (File copy)

Please return this signed page to your Manager to confirm you have read and understood the NZALS Acceptable **Internet and Email Use** Policy.

I have read and understood the NZALS Policy on Acceptable Internet and Email Use, and agree to abide by this Policy.

_____

Name

_____ _____

Signed Date