DATA SECURITY & PRIVACY

MANUAL NAME	ICT	**DATE ISSUED**	31 March 2021
POLICY NUMBER	01	**REVISION DATE**	31 March 2023
VERSION NUMBER	02		
DOCUMENT OWNER	Finance Manager		
APPROVED BY	Chief Executive		

Objective

The purpose of this Policy is to describe how SLSNZ maintains data security and the privacy of individuals in accordance with the Privacy Act 2020 (the Act) and the Information Privacy Principles under the Act.

Scope

This Policy applies when the SLSNZ collects, stores, uses, or discloses data and in particular the personal information of any individual.

Definitions

Personal information means information about an identifiable individual, such as an employee, member or donor.

SLSNZ will only collect personal information if that information is necessary for the purposes of SLSNZ's functions and activities.

Types of personal information SLSNZ might collect include:

- An individual's:
  - name, address, and contact details;
  - emergency contact details;
  - educational background, training records, job title, employment history, areas of expertise;
  - remuneration, benefits, bank details;
  - performance history, performance appraisals, misconduct complaints;
  - lifeguarding qualifications and any relevant health information
- Information relating to suitability for employment with or membership of SLSNZ.
- Records of correspondence between an individual and SLSNZ.
- Other personal information provided by the individual to SLSNZ.
- Any other information that is necessary to facilitate the purposes of SLSNZ's functions and activities.

SLSNZ Surf Life Saving New Zealand

ICT Information and Communication Technology

Related policies and procedures

HR Policies

Exceptions

There are no exceptions to this policy.

Responsibilities

- It is the responsibility of the Finance Manager to ensure that ICT data storage solutions provided are robust and meet industry best practice.
- It is the responsibility of the Senior Management team to ensure their employees are aware of, and comply with, this policy.

Policy

1.1 Access to data

1.1.1 Only authorised SLSNZ employees, contractors, and volunteers may have access to SLSNZ data.

1.1.2 The Finance Manager (or their delegate) can authorise data access, and each individual provided with data access must sign a user agreement.

1.1.3 Where access is authorised an individual will be provided with a user name and password.

1.1.4 Logon details should not be shared with any other individual and no user may allow another person to access the server using their logon.

1.1.5 Where an authorised individual is logged onto SLSNZ systems, they shall not allow any other individual to use their device, except with their direct supervision.

1.2 Passwords

1.2.1 In order to access the systems each user will be required to create a unique password.

1.2.2 This password must be a minimum of eight characters, contain a mixture of upper and lower case and at least one non alpha numeric character. It should also not be used by the individual to access any other system.

1.2.3 Following industry best practice SLSNZ will require all passwords to be updated regularly.

1.2.4 On no account must individuals write down their password or share their password with another individual (except the Finance Manager or their delegate or Lantech) as this can put the security of the system at risk.

1.3 Use of USB drives (memory sticks)

1.3.1 In order to ensure the security of SLSNZ data no USB drives can be taken offsite holding any confidential information pertinent to SLSNZ, their policies, procedures, or operations.

1.3.2 Users who wish to work from an offsite location must request VPN access from the Finance Manager, but may not use USB drives to transfer data to another location.

1.3.3 Any individual using a USB drive on SLSNZ system must ensure it is free from viruses prior to use.

1.4 Personal ICT devices

1.4.1 In order to ensure the security of the network, personal ICT devices, including cell phones, laptops, mp3 players, are not to be connected to the SLSNZ network, either through a computer, or via the wireless network unless permission is granted by the Finance Manager.

1.5 Virus Scans

1.5.1 SLSNZ will ensure that all machines are monitored by anti-virus software, and that this is kept current with the latest virus definitions.

1.6 Backup of Data & Disaster Recovery

1.6.1 SLSNZ will ensure that data is backed up electronically to an offsite facility on a daily basis.

1.6.2 Individual machines are backed up to the server on an hourly basis allowing full data recovery for individuals should a file corrupt

1.6.3 Disaster recovery simulations are run regularly to ensure that a full system restore can occur

1.7 Ownership of Data

1.7.1 Any material held on an SLSNZ machine becomes the property of SLSNZ – this includes all emails, images, and documents, and may be monitored by SLSNZ to ensure data integrity

1.8 Data Privacy

1.8.1 Methods of collection of personal information

SLSNZ will aim to collect personal information directly from the individual concerned. Some personal information may also be collected from other sources, such as:

1.8.1.1 SLSNZ member clubs
1.8.1.2 Third party service providers
1.8.1.3 Publicly available sources, and
1.8.1.4 Other sources authorised by an individual (such as referees during recruitment)

1.8.2 If an individual refuses to provide their personal information, or if SLSNZ is otherwise unable to collect an individual's personal information, SLSNZ may not be able to carry out its functions or discharge its obligations to that individual. In such circumstances, SLSNZ will inform the individual of the consequences of not being provided with the personal information.

1.8.3 Purposes of collection of personal information.

1.8.3.1 SLSNZ collects personal information for a variety of purposes connected with its functions and activities. SLSNZ will only use personal information for the purposes for which it was collected (or directly related purposes), or for any other purposes authorised by the individual concerned, or as required by law.

1.8.3.2 Purposes of collection can include:

a. Verifying the identity of individuals
b. Communication with individuals
c. Providing information on products and services
d. To process applications for recruitment or membership
e. Keeping records of member qualifications and activity
f. Administering payroll
g. To collect money owed or facilitating donations
h. To undertake research
i. Fulfilling the legal and regulatory obligations of SLSNZ
j. Purposes connected to the administration of SLSNZ
k. To protect and/or enforce our legal rights and interests, including defending any claim
l. Any other purpose authorised by the individual or the Act

1.8.3.3 Before using personal information, SLSNZ will take reasonable steps to ensure the information is accurate, up to date, complete, relevant, and not misleading.

1.8.4 Disclosure of personal information

1.8.4.1 SLSNZ may disclose personal information where disclosure is one of the purposes for which is was collected (or a directly related purpose), or to the individual concerned or to a third party if the individual has authorised that disclosure, or as required by law.

1.8.4.2 SLSNZ may disclose personal information to:

a. Legal and regulatory authorities (such as IRD);
b. Third-party professional providers (such as accountants, auditors, and lawyers);
c. Third-party providers of products and services to SLSNZ (such as pay-roll providers, KiwiSaver providers, IT system suppliers, information management providers);
d. Other third parties for anonymised statistical purposes;
e. Relevant officers of member clubs;

f. Any person authorised by the individual.

1.8.4.3 The recipients of disclosed personal information may be located outside of New Zealand. Some of the countries to which personal information is disclosed may not have privacy laws that provide comparable safeguards to those in the Act. In these cases, SLSNZ will either:

a. Take steps to ensure that the recipient of any personal information protects the personal information in a way that provides comparable safeguards to those in the Act, or otherwise complies with the Act, or

b. Obtain the authorisation of the individual concerned to the disclosure, after informing the individual that their personal information may not be protected by the recipient with comparable safeguards to those in the Act.

1.8.4.4 Before disclosing personal information, SLSNZ will take reasonable steps to ensure the information is accurate, up to date, complete, relevant, and not misleading.

1.8.5 Storage of personal information

1.8.5.1 SLSNZ will take steps to ensure personal information is protected by reasonable security safeguards against unauthorised use, modification or disclosure, or loss, or misuse.

1.8.5.2 SLSNZ will not keep personal information for longer than is required for the purposed of which it was collected.

1.8.6 Notifiable privacy breaches

1.8.6.1 A privacy breach occurs when personal information held by SLSNZ is accessed, disclosed, altered, lost, or destroyed without authority or by accident. A privacy breach also occurs when SLSNZ is prevented from accessing personal information that the SLSNZ should have access to.

1.8.6.2 If a privacy breach occurs and SLSNZ believes this has caused, or is likely to cause, serious harm to any individual, SLSNZ will notify the affected individual(s) as soon as possible. There are certain circumstances under the Act where notification may be delayed or not required.

1.8.6.3 If a notifiable privacy breach occurs, SLSNZ will also notify the Privacy Commissioner as required by the Act.

1.8.7 Access and correction

1.8.7.1 Individuals have a right to access to their personal information and to request that any inaccuracies are corrected. Individuals may request access to or correction of their personal information by submitting their request in writing to SLSNZ. SLSNZ will consider the request and will respond as soon as reasonably practicable by not later than 20 working days from the date the request is received.

1.8.7.2 Individuals have a right, at any time, to provide SLSNZ with a statement of the correction sought and to request SLSNZ attach that statement to their personal information. If the correction sought is not made, SLSNZ will take reasonable steps to attach that statement to the individual's personal information so that it is always read with the personal information.

1.8.7.3 There are certain circumstances where SLSNZ may not be required or permitted to allow an individual to access or correct their personal information. In some situations, SLSNZ may grant access to part, but not all, of the personal information requested. SLSNZ will inform the individual of the reasons for refusing their request for access (or part of their request for access) or correction.

1.8.8 Complaints

1.8.8.1 Individuals who have concerns or complaints about the privacy of their personal information should contact the Finance Manager.

1.8.8.2 Individuals may also complain to the Privacy Commissioner if they believe an action of SLSNZ may be an interference with their privacy.

Changes to this policy

SLSNZ may vary, replace, withdraw or not apply this policy at its absolute discretion.

Attachments
SLSNZ Staff ICT User Agreement.

References

Review
This policy will be reviewed biannually, and monitored as part of the internal control system.

SLSNZ STAFF ICT USER AGREEMENT

PERSONAL USE

1. SLSNZ provides ICT networks and equipment for work related activities and personal use should be kept to a minimum;
2. Personal files must not be stored on the network, but may be held on the local desktop. SLSNZ takes no responsibility for the loss of personal files stored in this manner.

ACCESS

3. Staff will be provided with a password to access SLSNZ systems – on no account should this password be shared with any other individual;
4. Staff should not allow unauthorised individuals access to SLSNZ systems, without their direct supervision;
5. Staff may not install software on their devices, or access the network with a personal device, without the express permission of the Finance Manager.

WEBSITE USE

6. Internet use will be monitored and SLSNZ reserves the right to limit web use on an individual basis;
7. Accessing illegal, or immoral websites, will result in the removal of all internet privileges and may result in disciplinary action.

EMAIL USE

8. Emails sent from an SLSNZ email account may be interpreted to be the opinion of SLSNZ so where personal opinions are expressed this should be clearly stated;
9. Using the SLSNZ email account to organise personal business is not acceptable;
10. Email use will be monitored and SLSNZ reserves the right to access the email account of any individual;
11. Use of email to bully or harass other staff, or to forward inappropriate content, will be investigated and may result in disciplinary action.

I have read and am aware of the obligations and responsibilities outlined in the Surf Life Saving New Zealand ICT Policies, and agree to follow them. I understand that apparent breaches of this agreement will be investigated and could result in disciplinary action up to, and including, dismissal.

Name: _____

Signature: _____ Date: _____