Privacy Policy

Created May 2021

Policy Purpose

This policy will:

- Set out the principles which are used by (Volunteer Service Abroad) VSA to collect, store, use and disclose personal information.
- Ensure that all VSA staff and contractors have a clear understanding of, and remain compliant with, the principles regarding the collection, protection, storage, access, distribution and sharing of personal private information relating to both staff and customers outlined in the Privacy Act 2020.
- Ensure VSA maintains adequate security safeguards to assure the privacy of information relating to staff, volunteers, stakeholders (including members and donors), and other individuals.
- Ensure VSA has a Privacy Officer with specific responsibilities in accordance with the Privacy Act 2020.
- Ensure VSA has a Privacy Statement accessible to visitors to the VSA website, and stakeholders.

Application

This is a Volunteer Service Abroad Te Tūao Tāwāhi operational policy, and it relates to all VSA staff and contractors working within New Zealand in accordance with the definitions contained in the Privacy Act 2020. It is expected that staff working in overseas posts will observe the requirements set out in this policy with respect to information contained within VSA systems.

VSA operational policies will be reviewed and amended as necessary with reasonable notice given to staff, and the union. Any material changes will follow a consultation process.

This policy should be read in conjunction with the VSA Code of Conduct and the Information Systems Acceptable Use policy.

Failure to comply with this policy (and any related instructions) may result in disciplinary action being taken, up to and including dismissal.

Policy Content

VSA uses personal information to conduct a range of day-to-day operations across VSA's business. This information is made available to staff, contractors, and other approved people for business purposes only. At times information is verified and shared with external government agencies and/or in-country organisations.

VSA is committed to ensuring that personal information is managed appropriately, and we strive to uphold good privacy standards in the collection, storage and use of personal information. Personal Information will only be accessed by those with authorised access to do so and only for the purpose of conducting VSA's business.

Information Privacy Principles

The collection, storage, use and disclosure of personal information is governed by the Privacy Act. In particular, section 22 sets out 13 information privacy principles (IPPS). VSA must comply with these IPPs. Many of the IPPs have exceptions to them, therefore it is important to refer to the requirements in full in the Privacy Act when considering their scope, but below is a summary:

IPP 1:	VSA must only collect personal information if it is necessary for a lawful purpose connected with a function or activity of VSA. Unless there is a lawful reason not to, VSA will make people aware of the collection of information, our purpose for doing so, and their rights to access and correct that information.
IPP 2:	VSA must only collect personal information directly from the individual concerned, or their appointed representative.
IPP 3:	When it collects information, VSA must take reasonable steps to ensure the individual knows when it is being collected, inlcuding: • the purpose of the collection, • the intended recipients of the information • if the information is required by law • which agency holds the information • whether the information is voluntary or mandatory • any consequences if the information is not provided • the individuals right to access and correct their personal information.
IPP 4:	VSA must collect personal information by lawful means and in a fair, non-intrusive manner.
IPP 5:	VSA must use reasonable safeguards to ensure that personal information is protected against loss, theft, unauthorised access, disclosure, or other misuse.

	VSA will keep physical documents secure when there is a business need to take them outside of VSA premises, and no technical solution is applicable. VSA will keep electronic personal information secure by ensuring its data storage is protected from external sources, maintaining regular back up of data to secure storage and applying good practice for information security management. VSA may use cloud computing services to manage and store information. Where used, VSA will ensure that cloud computing services meet all applicable New Zealand government security requirements.
IPP 6:	Individuals are entitled to request access to personal information held about them. Requests for information will be processed by VSA in accordance with the Privacy Act guidelines. In particular, VSA will: • acknowledge a request for personal information or correction of information as soon as possible after receipt. • Respond to requests for personal information, or correction of information, as soon as is reasonably practicable (and within 20 days of the request being made unless extended under the Privacy Act). • Notify the requestor, in the case of a request for correction of personal information, whether the information has been (or will) be corrected, and if not, the requestors right to provide a statement of correction to be attached to the information.
IPP 7:	Individuals are entitled to request that information held about them be corrected.
IPP 8:	VSA must take reasonable steps to ensure that personal information is accurate, current, complete, relevant, and not misleading, before using it.
IPP 9:	VSA must not keep the information for longer than needed for the purposes for which it may be lawfully used.
IPP 10:	VSA must not, in most cases, use personal information obtained in connection to one purpose, for another purpose, unless: • The source of the information is publicly available • The use of the information for the other purpose is authorised by the individual concerned • The purpose for which the information to be used is in connection with the purpose it was originally obtained • The information is in a form whereby the individual is not identified, and it is being used for statistical purposes and will not be published in a form where the individual's identity could be discovered.
IPP 11:	Personal information held by VSA must not, in most cases, be disclosed to another person or organisation, unless VSA has reasonable grounds to believe: • It is lawful to do so • That the disclose is authorised by the individual • That the information to be used is in a way the individual is not going to be identified.

	If it is unclear whether an individual may or may not be identified, VSA will act conservatively and not release the information until permission for its use has been granted by the individual to whom it relates.
IPP 12:	VSA must not disclose person information to a foreign person or entity that is not subject to the Privacy Act or comparable safeguards, unless VSA has obtained authorisation from the individual concerned.
IPP 13:	VSA must not assign a unique identifier to an individual unless it is necessary to carry out its functions. VSA does assign a unique identifier to members and other people in e-Tapestry.

Reasons for Refusal to Provide Information

VSA staff may receive requests for information. At times it may be inappropriate or unlawful to provide this information to the person or agency making the request.

VSA may refuse to provide information in the following situations, which are outlined under section 46 Privacy Act 2020:

- Where relatives or friends ask for information (unless the person concerned has provided their express written permissions to release information)
- VSA will not disclose reference check information comments to candidates as this is evaluative material compiled solely for the purpose of determining their suitability, eligibility or qualification for a specific role (both volunteer or internal).
- VSA will not disclose personal information that would breach legal privilege.

VSA Privacy Officer

The VSA Privacy Officer role rests primarily with the Director, HR and Volunteer Services, and includes responsibilities as follows:

- Ensures that staff remain compliant with the Privacy Act 2020 with respect to how they manage employee, volunteer, customer, supplier, and other stakeholder information.
- Manages any queries or complaints about privacy from customers, staff, or volunteers.
- Alerts the Senior Leadership Team, or the CEO specifically, to any risks that may arise around security of personal information.
- Provides or arranges training for staff on Privacy Act requirements
- Provides advice to managers on how to ensure VSA's business practices comply with privacy requirements, and on any privacy impacts where business practices are changing.

- Liaises with the Privacy Commissioner if necessary, for investigations, where there is an actual or perceived breach of privacy.
- Liaises with the Director Stakeholder Engagement to ensure that communication regarding any privacy breach is managed in accordance with VSA brand and communication guidelines.

If the primary Privacy Officer is unavailable, the Director Stakeholder Engagement will assume responsibility for the Privacy Officer role.

The Privacy Officer can be contacted at **privacy@vsa.org.nz**

Privacy incidents

A privacy incident includes an actual privacy breach, a potential privacy breach, or a near miss.

A privacy breach occurs when there is an unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of personal information. A privacy breach can also include an action that prevents the agency from accessing the information on either a temporary or permanent basis.

A potential privacy breach occurs where an IPP might have been breached, but it is not known if an actual breach occurred.

A near miss is where an action could have resulted in a breach but ultimately the breach does not occur.

All privacy incidents (actual and potential breaches or near misses) discovered by staff should be notified to their immediate manager. Managers are responsible for managing the response to the privacy incident in accordance with VSA's **Privacy Incident Guidelines**.

VSA's **Privacy Incident Reporting Form** should be completed as soon as possible. This will be provided to VSA's Privacy Officer who will advise further on the management of the privacy incident. This may include the Privacy Officer or the CEO notifying the incident to the Office of the Privacy Commissioner where required under the Privacy Act or if notification is considered necessary in the interests of transparency.

Reporting Problems or complaints

Staff or contractors must report any suspected or actual breaches of privacy to the Privacy Officer as soon as they become known. This will enable relevant staff to address the issue and also to minimise any impact on VSA. This may include, but is not exclusive to, planning for reputational damage, fixing

security issues, and/or liaising with the Office of the Privacy Commissioner and other relevant agencies.

Where any staff or contractors become aware of a privacy complaint made by an individual to VSA or to the Office of the Privacy Commissioner, VSA's Privacy Officer must be notified before any action is taken on behalf of the organisation.

Further Obligations

VSA will regularly review its business processes that relate to the collection, access, storage, use and destruction of personal information so they remain relevant and reflect good practice.
VSA will train and inform its staff and contractors of this policy and ensure the information privacy principles are applied when fulfilling their work within VSA.
VSA will endeavour to protect the privacy of staff, volunteers and other stakeholders.

Employees and Contractors responsibilities

Staff and contractors are responsible for:

- Reading this policy and adhering to the obligations outlined in it
- Attending mandatory training covering privacy obligations
- Following processes for reporting actual or potential breaches of privacy as outlined in this policy.

Manager's responsibilities

Managers are responsible for:

- Ensuring all staff and contractors have read and understood the requirements outlined in this policy, and how it relates to the work they perform.
- Registering staff for mandatory Privacy Training covering privacy obligations.
- Ensuring the processes relating to gathering, storing, and sharing of personal information complies with this policy
- Where processes require amending, this is done in consultation with the Privacy Officer
- Ensuring that staff and contractors are aware of the reporting process for actual or potential breaches of privacy.

References / CID Code of Conduct alignment

CID – This policy supports C.1.1 Transparency (obligation 2); C.3.4 protection of donors (obligation 1)

Legislation – Privacy Act 2020

Guidelines from: Office of the Privacy Commissioner

Approval

Function	Role
Policy Approver	Chief Executive
Policy Owner	Director, HR and Volunteer Services
Contact Person	HR Coordinator

Signed:

Date:

26 May 2021

Stephen Goodman

Chief Executive Officer

Volunteer Service Abroad