



Pacific Assist
Inspiring Self-reliance

Privacy

Policies and Procedures

2020

Version Number: 2

Approved by Board on: 15/01/2021

Last updated: November 2020

Scheduled review date: November 2022

Pacific Assist Privacy Policy

At Pacific Assist we are committed to ensuring the confidentiality and security of your personal information. We are bound by the Privacy Act and the Australian Privacy Principles (APPs). This Privacy Policy is intended to be a general statement that describes how we collect, use, and process personal information you provide on our website and through other means.

What is personal information?

Personal information is information or an opinion about an individual:

- Whether or not the information or opinion is true or not; and
- Whether the information or opinion is recorded in a material form or not.

Collecting sensitive information

We will not collect sensitive information¹ about you except:

- For health information if you register to volunteer
- When required to by law and requested to by regulatory bodies, government agencies, law enforcement bodies and courts
- To comply with national and international child protection, vulnerable peoples, and ant-terrorism laws and regulations

If you register to volunteer, we will send you a volunteer registration form that includes a request for basic health information necessary to assess your suitability to participate in specific projects, and to manage your safety and well-being during the period of your service as a volunteer. We do not collect health information without your written consent. Your health information will only be disclosed to a service provider or organisation in accordance with the *Information Sharing and Disclosure* statement below.

To comply with child protection laws and policies, we also collect and keep on file a copy of state specific Working with Children cards for all directors, executive officers, personnel, members, volunteers, partners, and service providers when they have any interaction with children as part of their role or involvement with Pacific Assist.

¹ Sensitive information is defined as racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; criminal record; or health information.

Ways we collect personal information

Pacific Assist collects personal information if you:

- Provide a service to us
- Partner with us
- Offer to donate supplies and equipment
- Volunteer your services
- Recommend a project
- Make a financial donation
- Make an enquiry
- Participate in a Pacific Assist project

We may collect your information in several ways:

- Directly from you (for example, when you visit our website, complete a form, or contact us by telephone)
- From publicly available sources or information (for example, your organisation's website)

Why we collect your personal information

We collect personal information from all directors, executive officers, personnel, volunteers, partners, participants, and service providers for some or all of the following reasons as applicable:

- To comply with national and international child protection, vulnerable peoples, and ant-terrorism laws and regulations
- To engage with them to effectively collect and/or deliver donated supplies and equipment, determine potential projects, process financial donations, enable them to participate in our projects or provide them with information about our projects, to conduct project research and evaluation, provide them with a tax receipt at tax time, enable them to participate in or invite them to participate in our fundraising efforts, gain an understanding of their communication needs, and perform research and analysis to improve the way in which we engage with them as an interested party
- To carry out our projects in pursuit of our stated charitable purposes:

- Foster educational development
- Promote health & well-being
- Provide humanitarian aid
- Promote economic development

If we do not collect this information from you, we may not be able to meet our legal obligations, fulfil your requests, process your donation, enable you to volunteer or participate in our projects, partner with you, engage your services, and/or effectively communicate with you.

Information sharing and disclosure

We regard your personal information as confidential and do not sell it to anyone. We do not share your personal information with other parties except in the following circumstances (or in other instances where we specifically inform you and obtain your prior consent):

- To undertake management and administration functions. For example, we may provide personal information to third parties for their use in performing internal functions on our behalf such as project management, payment processing, maintenance, security, data analysis, hosting, and so forth. In such instances, the providers will be contractually required to protect personal information from additional use (including for marketing purposes) or transfer in accordance with this Privacy Policy.
- When required to by law and requested to by regulatory bodies, government agencies, law enforcement bodies and courts
- To comply with national and international child protection, vulnerable peoples, and ant-terrorism laws and regulations

Anonymity/Nickname

You have the right to ask that we do not record your real name. Sometimes we may require your real name, for example, if you wish to be a volunteer, partner or service provider.

Third-Party Data

Where local law permits, you may submit personal information, including contact information about someone other than yourself (in other words, a third party) to allow us to contact that person, make a delivery, or otherwise meet your request. The information collected will be used solely to facilitate your request. When providing personal information about anyone other than yourself, you must first obtain the other person's informed consent if his or her consent is legally required.

If you submit personal information about someone else, please show them a copy of this policy so that they may understand the way their personal information may be used or disclosed in connection with your dealings with us.

Children's Privacy

We do not knowingly collect information from minors under the age of 18. If a minor desires to volunteer, they can only do so with the prior written and informed consent of their parent or guardian in compliance with applicable law. We strongly recommend that minors under the age of 18 ask their parents for permission before sending any personal information to anyone over the Internet, and we encourage parents to teach their children about safe Internet use practices.

Protection of Information

All personal information collected from individuals will be securely stored by Pacific Assist and protected from unauthorised use or access.

We use technical and organizational measures to protect the personal information we receive against loss, misuse, and unauthorized alteration and to protect its confidentiality. We regularly review our security procedures and consider appropriate new security technology and methods. We also use current encryption technology to encrypt the transmission of data on our log-in pages. However, because we cannot guarantee the complete security of these encryption technologies, please use caution when submitting personal information online.

We do not collect credit card information. Credit card transactions are processed via PayPal through their website. Once the transaction is completed, PayPal provide a confirmation email and receipt. PayPal maintain technical, physical, and administrative security measures

designed to provide reasonable protection for Personal Data against loss, misuse, unauthorized access, disclosure, and alteration. Their security measures include firewalls, data encryption, physical access controls to their data centres, and information access authorization controls. For further information about how PayPal manages personal information refer to their privacy policy located on their website.

Passive Data Collection

Tracking Technologies, Cookies, and Clear GIFs. When you visit any of our sites, our servers or filtering systems may collect information that your web browser sends any time you visit a website. This information may include but is not limited to your browser type, your operating system, your language preference, any referring web page you were visiting before you came to our site, the date and time of each visitor request, and information you search for on our sites.

We also use cookies and clear GIFs to collect information. A cookie is a small bit of data used to transfer information to either your computer's hard drive or your web browser for record-keeping purposes. A cookie serves as a sort of label that allows our sites to recognize your web browser when you return to our sites. A clear GIF (also known as a web beacon) is used in combination with cookies to help us understand how visitors interact with our sites. A clear GIF is typically a transparent graphic image placed on a website. The use of clear GIFs allows us to monitor your actions when you open a web page and makes it easier for us to follow and record the activities of recognized browsers. For example, using clear GIFs, we can track the path of page visits on a website and monitor aggregate usage and web traffic routing on our sites.

We collect this information to better understand how you use and interact with our sites in order to improve your experience. We may also share this information with our employees, contractors, service providers, and affiliated entities in accordance with the *Information Sharing and Disclosure* statement above.

You can change your web browser settings to stop accepting cookies or to prompt you before accepting a cookie from the sites you visit. If you do not accept cookies, however, you may not be able to use some sections or functions of our sites.

To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit <http://www.allaboutcookies.org>. To opt out of being tracked by Google Analytics across all websites visit <https://tools.google.com/dlpage/gaoptout>.

Third-Party Links

We are not responsible for the privacy practices or content of any third-party sites we reference or provide links to. For your own protection, you should review the policies of other sites to ensure they meet your personal privacy expectations.

Policy Compliance and Questions Regarding the Privacy of Personal Information

You can request access to your personal information, request a correction to your personal information, and/or make a privacy complaint. If you have any enquiries in relation to personal information and/or privacy, or you wish to unsubscribe from our news updates or newsletter please contact:

Clive Haydon
Pacific Assist
Level 4 / 420 Collins Street
Melbourne VIC 3000
Email: clive@pacificassist.org
Phone: 0427 681 232

For more information about the Australian Privacy Principles or to make a complaint directly to the Privacy Commissioner, please visit the website of the Office of the Australian Information Commissioner <http://www.oaic.gov.au/> .

Future Changes to Privacy Policy

We regularly review this Privacy Policy and may change, modify, add, or remove portions as needed. If we change this Privacy Policy in ways that affect how we use your personal information, we will notify you here or in a notice on our home page. We will also update the revision date at the bottom of the Privacy Policy. We encourage you to check this Privacy Policy from time to time to remain informed of any changes.

Updated 06 November 2020.

Procedures

To meet our obligations to protect the confidentiality and security of the personal information we collect, all Pacific Assist personnel, volunteers, partners, and service providers are to apply the following procedures as they apply to their roles and responsibilities.

P Drive

Pacific Assist's computer information system is hosted by Frontier Financial Group (FFG). As a licensed financial services operator, FFG is required to meet stringent personal information protection and security standards. FFG contract the management and security of the system to Vixtro Pty. Ltd. Vixtro provide the latest technical and organizational measures to protect the integrity of the system. To ensure the integrity of records kept and utilised by Pacific Assist, Vixtro have created a separate drive within the FFG system dedicated solely to Pacific Assist. The dedicated Pacific Assist drive is called the P Drive. This folder sits outside of FFG's folder structure. The Pacific Assist folder is password protected and only the administrator (Vixtro Pty. Ltd.), Richard McLean (Pacific Assist director) and Pacific Assist's projects manager have access to it. Access to anyone else should only be granted if it is deemed by the board of directors that access is necessary for the effective management of Pacific Assist and its operations. Access can only be obtained as follows:

- A request for access to the P Drive must be made in writing to the board of directors
- The board of directors must approve all requests for access to the P Drive
- The board of directors determine if access is limited to general information only, or if full access is granted including access to password protected personal information
- The decision of any request for access to the P Drive must be noted in the minutes of the meeting in which the decision was made. The note should include:
 - The name of the person receiving access
 - The reason access is being granted/not granted
 - The level of access granted (general or full)
 - The time period for which access is granted
- The projects manager will arrange and oversee authorised access to the P Drive in accordance with the decision of the board of directors

Information Categories

To manage and protect the personal information it collects, Pacific Assist divides personal information into four categories:

- Personal Information
- Sensitive Information
- Identification Documents
- Research Data

Personal Information

Personal information that is not sensitive information, identification documents, or research data should be managed as follows:

- Only directors, the projects manager, and project coordinators are authorised to collect and manage personal information on behalf of Pacific Assist
- Personal information must be collected according to project plan policies and procedures (as a minimum, project plan policies and procedures must conform to Pacific Assist's privacy, record keeping, and research and ethics policies and procedures)
- Transfer all hardcopy information into digital format by scanning documents and saving them as PDF or other file types
- Confirm that the information has been accurately and completely saved in PDF or other file types (save files in accordance with Pacific Assist's recording keeping polices and procedures)
- Except for personal documents that are to be returned to the provider, shred all hardcopy information ensuring all personal information is destroyed

Sensitive Information, Identification Documents, and Research Data

Sensitive information, identification documents, and research data should be managed as follows:

- Only directors, the projects manager, and project coordinators are authorised to collect and manage sensitive information, identification documents, and research data on behalf of Pacific Assist
- Sensitive information, identification documents, and research data must be collected according to project plan policies and procedures (as a minimum, project plan

policies and procedures must conform to Pacific Assist's privacy and record keeping policies and procedures and the research and ethics policies and procedures)

- Transfer all hardcopy information into digital format by scanning documents and saving them as PDF or other file types
- Confirm that the information has been accurately and completely saved in PDF or other file types (save files in accordance with Pacific Assist's recording keeping policies and procedures)
- Password protect each file (passwords should be recorded in the Lastpass password management application)
- Research data files should be handled in accordance with Pacific Assist's research ethics and practice policies and procedures and individual research plans
- Research data should only be accessible to the lead researcher and anyone they provide written authorisation to
- Except for personal documents that are to be returned to the provider, shred the hardcopy information ensuring all sensitive information, identification documents, and research data are destroyed
- Once information has been accurately and completely saved to PDF or other file types within the P Drive, delete emails, text messages, files stored on external hard drives, cloud servers and/or shared drives that contain sensitive information, identification documents, and research data (unless research data is being stored on an approved and secure research platform)

Non-digitised Hardcopy Information

Personal information, sensitive information, identification documents, and research data that cannot be digitised should be managed as follows:

- Only store hardcopy personal information, sensitive information, identification documents, and research data when it is impossible to digitise it
- Store all hardcopy information in a locked filing cabinet in accordance with Pacific Assist's recording keeping policies and procedures
- Only Richard McLean (Pacific Assist director) and Pacific Assist's projects manager have access to the filing cabinet. Access to anyone else should only be granted if it is deemed by the board of directors that access is necessary for the effective management of Pacific Assist and its operations. Access can only be obtained as follows:

- A request for access to the filing cabinet must be made in writing to the board of directors
- The board of directors must approve all requests for anyone else to access the filing cabinet
- The board of directors determine if access is limited to general information only, or if full access is granted
- The decision of any request for access to the filing cabinet must be noted in the minutes of the meeting in which the decision was made. The note should include:
 - The name of the person receiving access
 - The reason access is being granted
 - The level of access granted (general or full)
 - The time period for which access is granted
- The projects manager will arrange and oversee authorised access to the filing cabinet in accordance with the decision of the board of directors

External Hard Drives

External hard drives and USBs should be managed as follows:

- When necessary, external hard drives and USBs can be used to transfer data from an external source to the P Drive
- Ensure sensitive information, identification documents, and research data is password protected before utilising an external hard drive to transfer it to the P Drive
- Do not store sensitive information, identification documents, and research data on external hard drives beyond the time necessary to transfer it from the source device to the P Drive
- Once information has been accurately and completely saved to PDF or other file types within the P Drive, delete files from external hard drives that contain sensitive information, identification documents, and research data

Training

The projects manager provides privacy, record keeping, and research and ethics policy and procedures training to project coordinators.