

Purpose

This policy explains how Pacific Link Housing (PLH) and its wholly owned subsidiaries (PLH Group) comply with our legal obligations to protect the privacy of personal information.

This policy also provides guidance on the types of information we collect and hold as well as, when we will disclose information held and how to gain access to your personal information (including to correct it).

Scope

This policy is relevant to all activities and the collection of personal information by the PLH Group.

Where Do We Collect Personal Information From and How

Personal information is information or an opinion about an individual whose identity is apparent or can reasonably be ascertained.

We aim to collect personal information we hold directly from the person the information is about. However, when this is not practical, personal information may come from applicants, tenants, members of tenants' households, job applicants, employees, directors, referring agencies, service providers (including health providers) volunteers, contractors, visitors, agencies, within the PLH Group and others that come into contact with the PLH Group.

How we collect information depends on whose information it is and the purpose we are collecting it for. Where practical, we will obtain personal information directly from the person it relates to. It can be collected using forms, emails, letters notes, SMS, conversation, meetings, financial transactions, CCTV, and monitoring activities. For example:

- We may collect information from the Police to maintain law and order in and around PLH Group owned and managed properties, where an emergency poses an imminent threat to life or property, in the investigation of an alleged criminal offence or breach, or to develop and implement crime prevention and community safety strategies.
- We operate CCTV systems in our office according to our Monitoring and Surveillance Policy, and at several property locations - refer CP21 CCTV Surveillance at PLH Properties Policy.

If the PLH Group receives information via an avenue it would not normally obtain personal information from (for example, where a complaint is made about a person), the information will only be held, used and/or disclosed if we could have collected it through normal avenues.

Personal Information We Collect

The PLH Group collects personal information that is relevant or necessary to conduct its business and related activities. Whilst the personal information we collect may change depending on whose information we are collecting and why, we generally collect and hold:

- **Personal information:** such as names, addresses, dates of birth, next of kin details, financial information, email addresses, photographic images and attendance records.
- **Sensitive information:** this may include details of nationality, country of birth, religious beliefs, languages spoken at home, family court orders and criminal records.
- **Health information:** medical records, information relating to disabilities, individual health care plans, and counselling reports.

Use of Your Personal Information

The PLH Group uses your personal information for the reason we collected it as it relates to the function or activity we undertake. This is known as the “primary purpose”. Broadly, our primary purpose for collecting personal information includes but is not limited to:

- Housing and related services (including NCAT, allocations and support provision).
- Maintenance contracting and works.
- Meeting the requirements of agencies at all levels of government (including reporting) under funding and other contracts.
- To meet our legal, regulatory and compliance obligations including in relation to safety, employees, tenants, child protection and duty of care obligations.
- Employees and volunteers – this includes training, employment, improving operations, developing programs and systems, research, advocacy (where possible, personal information is de-identified).
- Commercial activities – to run the business effectively including governance, administration, insurance and policy setting within the PLH Group (where it is not sensitive information).
- Property and community development activities.
- Marketing, promotional and fundraising activities – this includes newsletters, activities, community events and social media.

We may use your information for a secondary purpose where you have provided consent, or another exception applies. For example, such as being reasonably necessary for enforcement activities to be carried out on behalf of an enforcement body.

Disclosure of Your Personal Information

Disclosure of your personal information occurs when we give someone else access to it, or if we show another individual, organisation or agency. We may disclose your personal information if:

- It is the reason the information was collected.
- You would reasonably expect us to disclose this information in this way.
- We have a legal obligation to do so.
- Disclosing that information could prevent a serious threat to life, health or safety of an individual (or for public safety).
- Another exception applies under privacy legislation and principles.
- You have provided consent for us to disclose the information.

Parties we may disclose your personal information to are government agencies (including Centrelink), courts, tribunals, service providers (including service providers who may handle personal information on our behalf), police and law enforcement, emergency services, health services, real estate agents, business and support partners, contractors, advisors.

We may disclose personal information about an individual to overseas recipients in certain circumstances, such as storing information with a “cloud service provider” which stores data outside Australia. If we do this, we will take all reasonable steps not to disclose an individual’s personal information to overseas recipients by making sure:

- We have consent (which may be implied).
- We are satisfied they are compliant with Australian Privacy Principles or similar standards.
- Disclosure will likely lessen or prevent a serious threat to the life, health, or safety of an individual or to public safety.

Security and Security of Information

We store personal information in a variety of formats including on databases, third party databases, in hard copy files and on personal devices including laptop computers, mobile phones, tablets, cameras and other recording devices. We take all reasonable steps to protect the personal information we hold about you from misuse, loss, unauthorised access, modification or disclosure. These steps include:

- Restricting access to information on our databases on a need to know basis. Different levels of security and access are allocated to employees based on their roles and responsibilities.
- Ensuring all employees are aware that they are not to reveal or share personal passwords.
- Ensuring where sensitive and health information is stored in hard copy files that these files are stored in a secure filing room or locked cabinets.
- Implementing physical security measures to our office to prevent break-ins or unauthorised access.

- Implementing security systems, policies and procedures, designed to protect personal information storage on our computer networks.
- Developing and implementing human resources policies and procedures, such as email and internet usage, working from home, confidentiality and document security policies, designed to ensure that employees follow correct protocols when handling or transmitting personal information.
- Engaging third parties under contract terms that require them to restrict access to information and ensure adequate security measures are implemented.
- Personal information we hold that is no longer needed is destroyed in a secure manner, deleted or de-identified as appropriate, in accordance with legislative requirements. Please refer to our Data Governance Policy.

Data Breaches

Where a data breach occurs, the PLH Group will take all reasonable actions to minimise the impact of a data breach to those persons affected.

The PLH Group is required to notify individuals and the Office of the Australian Information Commissioner (OAIC) about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates. An eligible data breach arises when the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information,
- this is likely to result in serious harm to one or more individuals and
- PLH Group has not been able to prevent the likely risk of serious harm with remedial action.

Quality Assurance and Access to Your Information

We will take all reasonable steps to ensure that the personal information we collect, hold and use is relevant, accurate, current, complete, and not misleading.

In addition, you may request to see the information about you that we hold and use. However, there are rules and procedures on what you can access, when we can refuse to give you access, and your right to appeal.

You can also request that we amend data that is not accurate, up to date, incomplete, or misleading. Where we refuse to comply with your request, you have a right to appeal.

Contact Information and Complaints

To request access to your information, request correction of your information, make a privacy complaint or make an enquiry about PLH Group and your privacy, please contact our Privacy Officer:

Group Executive Manager, Legal Compliance & Risk
Pacific Link Housing
PO Box 1888
GOSFORD NSW 2250
02 4324 7617
info@pacificlink.org.au

Where you make a complaint, it will be acknowledged as soon as possible after we receive it, and we will aim to investigate and respond to the complaint within 30 days. This may include obtaining further information from you to support review of and response to, the complaint.

If you are unsatisfied with the outcome of your complaint, you may also raise your concerns with the Office of the Australian Privacy Commissioner or the NSW Privacy Commissioner.

Related Policies

CP20 Monitoring and Surveillance Policy
CP21 CCTV Surveillance at PLH Properties Policy
CP22 Regulatory Notifications Policy
CP44 Child Protection and Mandatory Reporting Policy
CP65 Data Retention Policy

Policy Owner	Group Executive Manager, Legal, Compliance & Risk
Approval Authority	Board
Approval Date	September 2024
Next Review	September 2027
Website published	Yes