



HLP Controls Pty Ltd
5/53 Argyle Street
South Windsor NSW 2756
ABN: 50 097 834 690
P: 1800 500 160 F: 1800 827 160
E: sales@hlpcontrols.com.au
W: www.hlpcontrols.com.au

Privacy Policy & Procedure

Table of Contents

About this policy	1
Overview	2
Adherence to APP	2
Collection of your information	2
Collecting sensitive information	2
Collecting information through our websites	3
Analytics	3
Cookies	3
Email lists, registrations and feedback	3
Social networking services	3
Passwords and protection	4
Electronic forms	4
Your cloud data	4
Email	5
Disclosure	5
- Credit card payment of account	5
- Data breach notifications	5
- Disclosure to service providers	5
- Disclosure of sensitive information	6
- Disclosure of personal information overseas	6
Quality of information	6
Storage and security of information	6
Building access	6
How to make a complaint	6
Contact	6
Staff Training	7
Attachment 1: APP Guidelines (Australian Privacy Principles)	8

About this policy

The *Privacy Act 1988* requires Companies to have a privacy policy. This privacy policy outlines the personal information and data handling practices of HLP Controls Pty Limited.

This policy is written in straightforward language. The specific legal obligations of HLP Controls when collecting and handling your personal information and data are outlined in the *Privacy Act 1988* and in particular in the Australian Privacy Principles found in that Act. We will update this privacy policy when our information and data handling practices change. Updates will be available on our websites.

Overview

We collect, hold, use and disclose information to carry out functions or activities within our Company (HLP Controls Pty Limited)

These functions and activities include:

- handling your name, address, phone number & email address information;
- holding these details on our Company server in MYOB;
- handling your credit card details when you give them to us to use to pay your invoices;
- accessing & handling details such as your ABN and credit reporting information when you open a credit account with us;
- holding your data-logged data on a secure cloud server;
- assessing suitable candidates for career opportunities within the HLP Controls.

Adherence to APP (Australian Privacy Principles)

A copy of the APP is attached to this procedure and is included in staff training carried out.

HLP Controls will always comply with all APP guidelines and directions to ensure security and privacy is maintained for our customers and their data as well as being protection of our Company.

Our staff's acknowledgement of this is through our staff training policy and the employee's signature of a copy of this procedure which is held in our employee files.

Collection of your information

At all times we try to only collect the information we need for the particular function or activity we are carrying out.

The main way we collect information about you is when you give it to us. For example, we collect personal information such as contact details when you:

- contact us to ask for information, to buy a product or pay an account over the phone (but only if we need it);
- ask for access to information HLP Controls holds about you;
- ask for access to password protected sections of the HLP Controls web sites;
- set up an account on the HLP Controls cloud server to store your data;
- apply for a job vacancy at the HLP Controls;
- make a complaint to us.

Collecting sensitive information

Sometimes we may need to collect sensitive information from you, for example, you may choose to pay your account via your credit card. This information will include all of the credit card details such as the number, name on the card, expiry date & CCV. We do not hold credit card information after it is used for the payment you authorised us to use it for.

Other information may be accessed by us when you complete and sign an account form in order for us to open a credit account for you or your Company. We access your credit information via our consumer credit reporting agency Equifax. You can access Equifax Privacy Policy on their web site www.equifax.com.au

Collecting information through our websites

HLP Controls has its own public websites. These are:

www.hlpcontrols.com.au

www.manlaw-bbq.com.au

www.geartracker.com.au

There are a number of ways in which we collect information through our websites.

Analytics

We use Google Analytics to collect data about your interaction with our website. Google Analytics is hosted by a third party. The sole purpose of collecting your data in this way is to improve your experience when using our web sites. No specific personal information on You is collected. The types of information collected that we are able to access and examine is all general in nature.

The types of data we collect with these tools include:

- demographic;
- language;
- country and city;
- system, browser, operating system and service provider;
- mobile operating system, service provider and screen resolution;
- search terms and website pages visited;
- date and time when website pages were accessed.

Cookies

Cookies are small data files transferred onto computers or devices by websites for record-keeping purposes and to enhance functionality on the website.

Our websites generally set the `_ga`: Google Analytics cookie

Most browsers allow you to choose whether to accept cookies or not. If you do not wish to have cookies placed on your computer, please set your browser preferences to reject all cookies before accessing our websites.

Email lists, registrations and feedback

We will collect information that you provide to us when signing up to mailing lists and registering for our email-outs, or when submitting feedback on our websites.

We control and manage our own data bases of contact information in-house, however we use MailChimp to send out email notifications. You can access MailChimp's privacy policy at www.mailchimp.com/legal/privacy/. When subscribing to one of our mailing lists, you will start to receive emailed information from us. We only send email to email addresses where we have your consent to do so. We do not buy email address lists from 'third parties'. We may also receive your information over the phone from you, via fax/email or through contact at a trade show event or other way. With your consent this contact information will also be added to our data base lists.

Should you not wish to receive our email-outs at any time, you can unsubscribe by clicking the 'Unsubscribe' button at the base of the email. Your details will then be removed from that email data base list.

Social networking services

We use social networking services such as Facebook and YouTube to communicate about our products, business and to post helpful videos. When you communicate with us using these services we may collect your information, but we only use it to help us to communicate with you. The social networking service will also handle your personal information for its own purposes. These services have their own privacy policies. You can access the privacy policies for [Facebook](#) and [YouTube](#) (a Google company) on their websites.

We also use a separate company to post on our social media sites on our behalf. Their policies can be accessed through <http://www.atomicdigital.com.au/>

We do not hold your personal information other than that which you have disclosed through your contact with us.

Passwords and protection

HLP Controls require all personnel to change passwords used for company software and websites bi-monthly.

Passwords are to be kept secure by the employee and are not to be shared with other employees (except Management) or people outside the Company.

On changing a password, the new password to be given to Management (in person or by phone – not via email).

Electronic forms

HLP Controls has electronic forms for completion on it's web sites.

When you submit a form using this service it is encrypted and sent to us as an email. We download the information when we open the email.

Your cloud data

When you activate an account to have your data, such as temperature and other records, held on our cloud server, we will hold this information for you for 2 years. Within this period you can access and download your information as many times as you require. Should you or your business or your legal and moral requirements require more than 2 years of data to be held, then you need to download your own data & store it yourself, for instance on a hard disk drive or flash drive before the 2 year period has ended.

The cloud server is held with IoTstream. Their privacy policy may be accessed through their web https://streamvue.io/others/privacy_and_policy

Deleting your stored cloud data

Once data has been stored for 2 years it will automatically be deleted.

Should your credit account become sixty (60) days in arrears of payment, or should you give us written notice of termination of our arrangement to store your data for you, we reserve the right to delete your stored data within seven (7) days.

Email

When you send us an email it is stored on our in-house server. The details are held, backed up and not deleted. We hold these details in case you have further queries or in case we need to refer back to your emailed information at any time.

This information is available for our staff to view via password protected access.

Disclosure

Common situations in which we disclose information are detailed below.

Credit Card Payment of Account

If you make a credit card payment for an account owed to HLP Controls, we will enter your credit card number, expiry date and CCV either into our in-house Westpac credit card terminal or we will enter the information into our secure payment gateway called EWay. Eway have their own privacy policy to show how the information is handled, this may be accessed at www.eway.com.au & click on the 'legal' tab. Westpac have their own privacy policy to show how the information is handled, this may be accessed at www.westpac.com.au & click on the 'privacy' tab. Paypal is also available for use for website purchases. The Paypal privacy policy can be accessed at www.paypal.com/au/home

Data breach notifications

We will not disclose personal information about you to anyone outside our Company, except for instance to a Government agency in the event of a breach, unless you agree, or would reasonably expect us to disclose such information.

If we have a data breach at HLP Controls either on our in-house server or on our cloud server we will inform you immediately that we are aware of the event. We will also notify the Office of the Australian Information Commissioner (OAIC) of the data breach and comply with any and all of their recommendations and requirements.

Such a data breach could include if a device containing our customer's information is lost or stolen, a database containing information is hacked, or information is mistakenly provided to the wrong person. Please note that HLP Controls do not store credit card information. We use the credit card details you give us for the purpose you have allowed and then destroy the details.

Disclosure to service providers

HLP Controls uses a number of service providers to whom we disclose information. These include providers that host our website servers, manage our IT and manage our payment gateways. You can access the privacy policies for the web site hosts at www.experiencedigital.com.au and www.sitesuite.com.au/privacy-statement

We only disclose information when you request that we do so or when you would reasonably expect us to do so. We only use secure sites for payment processing. These are detailed in 'Credit card payment of account' section in this document.

We use Geeks2U to manage our server and IT requirements. Their privacy policy can be viewed on their website www.geeks2u.com.au

Disclosure of sensitive information

We only disclose your sensitive information for the purposes for which you gave it to us or for directly related purposes that you would reasonably expect or if you agree.

Disclosure of personal information overseas

HLP Controls outsources some company functions to an overseas agency. The agency has strong protection procedures and policies in place for their workers and the worker solely works for HLP Controls. Their privacy policy may be viewed on their web site at www.remotecontrolbpo.com

Quality of information

To ensure that the information we hold is accurate, up-to-date and complete we:

- record information in a consistent format
- where necessary, confirm the accuracy of information we collect with you
- promptly add updated or new information to existing records when you advise us of a change

Storage and security of information

We take steps to protect the security of the information we hold from both internal and external threats by ensuring that our systems can only be accessed with a unique password. All of our staff have unique password access to our server.

When we no longer require your printed information

We destroy information in a secure manner when we no longer need it. For example, we generally destroy records by in-house shredding.

Building access

Only certain trusted staff members are allowed key access to our building. They use a unique password to deactivate the security system. The logs of who accessed the security system, date and time can be access by Management at any time needed.

How to make a complaint

If you wish to complain to us about how we have handled your information you should complain in writing to: liz@hlpcontrols.com.au.

If we receive a complaint from you we will determine what (if any) action we should take to resolve the complaint and will promptly report back to you with a resolution.

Contact

All of our contact information is available on our web sites.

Staff Training

All staff will be trained on hiring and again annually on the need for security and confidentiality in all customer and company dealings. Staff are to be aware of who they speak to both at work and privately and the information they give out to ensure that they do not breach any customer or company security or confidentiality whether written or unwritten.

Acknowledgement of this training and their adherence to this policy is through their signature on a copy of this procedure and is kept in their employee file.

Staff also sign a confidentiality agreement on hiring. This is held in their employee file.

Signed:



L Wallace
Manager

1 June 2020

To be reviewed each January by Management.

Reviewed:

Review date	Signature	Review date	Signature