

Privacy Policy:***Respecting your Privacy:***

Kelly Engineering and its related entities (“Kelly”) is committed to compliance with privacy laws and your privacy is important to it. This policy outlines the company’s personal information management practices that relate to:

- The kinds of personal information that it collects and holds;
- How it collects and holds the personal information;
- The purposes for which personal information is collected, held, used and disclosed;
- Your right to access personal information that is held and to seek the correction of such information;
- Complaint resolution process concerning a breach of the Privacy Act 1988 (Cth) (Privacy Act), the Australian Privacy Principles, or a registered APP code (if any).
- The likelihood of sharing or disclosing personal information to overseas recipients.

This policy is current as at 25th May 2018. From time to time Kelly Engineering may find it necessary to amend this Privacy Policy to reflect changes in law or the Company’s commercial activities.

The latest version of our Privacy Policy can be obtained by contacting us or visiting our web site at www.kellyengineering.com.au

The company is bound by the Australian Privacy Principles and its procedures regarding personal information are designed to ensure that your rights under the Australian Privacy Principles are protected and that your personal information is managed in an open and transparent manner. The entities to which this Privacy Policy relates are listed in the schedule at the end of this policy.

Openness

Kelly will be open and transparent about how it handles personal information, by:

- Telling you when personal information is collected, what it is used for and to whom it may be disclosed
- Giving you more detailed explanation of its Privacy Policy if you ask for it;
- Giving you access to personal information that it holds about you if you ask for it;
- Correcting personal information that it holds about you if you ask it to do so; and
- Erasing personal information that it holds about you if you ask it to do so.

You have the right to access and request the correction of personal information that we hold about you under the Australian Privacy Principles. If you are an EU citizen, you have the right to lodge a complaint with a Data Protection Authority (DPA). If there is a reason Kelly is unable to agree to a request for access to your personal information you will be advised of this in writing. Details of how to make a request for access or correction are set out at the end of this Privacy

COMMUNICATION**QM Section: 7.4****Privacy and Notifiable Data Breaches Policy**

Policy. You may be charged a small fee to cover any costs or expenses that are incurred to respond to your request, such as labour costs, photocopying costs or facsimile charges.

What Type of Personal Information does Kelly Collect?

The personal information collected is necessary for its normal business functions and activities.

The personal information may include;

- Your personal details such as your name, address, telephone numbers, email address,
- Identification information,
- All relevant purchase history and warranty data
- Financial information, including your payment history,
- Other information that could be used for marketing purposes.

Sometimes information is collected through selected agents. These agents are under an obligation to protect your privacy when they deal with your personal information.

We collect and retain personal information about individuals or companies that supply goods and services to us. This information is used for purposes related to the acquisition of goods and services by us and is not used for any other purposes.

Kelly keeps detailed information about current and former employees, including detailed payroll information. This type of information will in most cases be exempt from the Australian Privacy Principles. It also keeps personal information about persons who apply for employment (this information is not exempt). Personal information may be used to advise you of special offers and events that become available to customers.

We respect your privacy and will give you the opportunity not to receive this information when we collect your details or on occasions when we send such material to you. We continue to be bound by the SPAM Act 2003 (Cth) and the Do Not Call Register Act 2006 (Cth) if we undertake direct marketing and we will comply with the provisions of these Acts.

From time to time we may disclose credit information to a credit reporting body with your prior approval. Further details are given to you about this when you apply for payment terms.

To Whom Do We Disclose Personal Information?

Kelly Engineering does not sell or disclose the personal information that we hold to any person outside Kelly Engineering for direct marketing by that other person.

Personal information that we hold may be exchanged between different businesses within Kelly Engineering (as listed in the Schedule) or to other related parties. This disclosure is permitted by the Privacy Act.

Personal information that we hold may be disclosed to the agent that supplied goods to you. It may also be disclosed to agents or contractors who act on our behalf to collect debts or recover goods and to service contractors that provide service and support to our customers who help us to comply with our service and warranty obligations to you. Finally, we may also disclose personal information to our solicitors and accountants. The identity of any of these people may

COMMUNICATION**QM Section: 7.4****Privacy and Notifiable Data Breaches Policy**

change from time to time.

Personal Information Disclosed Outside Australia

Some personal information we collect may be disclosed to persons or our contractors, suppliers, representatives, dealers or agents that are outside Australia. This is dependent on your business and requirements, particularly with respect to the Australian Privacy Principles and Privacy Act. It is important to specifically advise if you do not wish to have your information stored overseas.

Management and Storage of Personal Information

When we collect personal information about you we do so by making a record of it.

We take active steps to protect the security of all records of personal information, including authentication of customers before disclosure of personal information. We expect our staff to comply with certain standards of behaviour and values when dealing with personal information. We train selected staff about the need to protect your privacy and we will regard breaches of the Australian Privacy Principles as serious matters. We maintain and retain personal information in both electronic and paper based records. Paper based records are kept securely away from the general public.

Our electronic records are kept in a number of secure systems with password protection and restricted access both internally and from external sources. We may keep personal information for up to 7 years or longer after the completion of a transaction for legal or taxation purposes. After that time, we will de-identify or destroy the personal information if we no longer need it.

We try to ensure that any personal information that we hold is accurate, complete and up to date. We do this by collecting as much information about a person as possible from the person during the initial contact. We will also update and correct your personal information if it is incorrect or when you request us to do so. Should we become aware that the information is inaccurate, incomplete or out of date we will correct that information, make a note on or amend the file, or in some cases delete it from our records.

Anonymity and Pseudonymity

There may be occasions where you wish to deal with us anonymously or using a pseudonym (i.e. a name, term or descriptor that is not your actual name). You may wish to deal with us in either of such manners where you want to make an inquiry as to the availability or price of a particular product, part or service that we offer, opening hours or for any other kind of inquiry for which your personal information is not required in order for us to respond meaningfully to your query. In these circumstances we will respond to your query without seeking to collect personal information about you. However, where it is impracticable for us to deal with you if you do not identify yourself, then we are not obliged to give you the option of dealing with us anonymously or using a pseudonym. We will tell you if we think that such a situation exists. If you choose not to provide us with personal information, then we may not be able to provide you with the product, part or service that you seek.

COMMUNICATION**QM Section: 7.4****Privacy and Notifiable Data Breaches Policy**

Contacting Us About Privacy Issues

If you wish to:

- Obtain more information about our Privacy Policy;
- Obtain a hard copy of this Privacy Policy or obtain it in another format;
- Obtain access to personal information that we hold about you;
- Request the correction of personal information that we hold about you;
- Request the erasure of personal information that we hold about you;
- Make a complaint because you believe that we have breached either your privacy the Privacy Act, the Australian Privacy Principles, the registered Credit Reporting Privacy Code, or a registered APP code that binds us;

then you may contact our Privacy Officer who will take reasonable steps to respond to your inquiry or complaint and will do so promptly (usually within 14 to 30 days). Our Privacy Officer's contact details are:

Kelly Engineering

Attention: The Privacy Officer

PO Box 100

Booleroo Centre SA 5482

Telephone: 08 8667 2253

Fax: 08 8667 2250

E-mail: office@kellyengineering.com.au

The Privacy Act requires that you first make your complaint to us in writing and that we are then given a reasonable time to respond to you (usually within 30 days). If you make a complaint to our Privacy Officer but you are not satisfied with the response that you receive you can then make your complaint to the Credit Ombudsman Service. The Credit Ombudsman Service independently and impartially resolves disputes between customers and participating members on matters including privacy. Their contact details are:

Credit and Investments Ombudsman Limited

PO Box A252

South Sydney NSW 1235

Telephone: 1800 138 422

Fax: (02) 9273 8440

Complaints Email: info@cio.org.auWebsite: www.cosl.org.au

COMMUNICATION
Privacy and Notifiable Data Breaches Policy

QM Section: 7.4

Alternatively, you may contact the Commonwealth Privacy Commissioner with your complaint. The contact details are:

The Office of the Australian Information Commissioner

GPO Box 5218

Sydney NSW 2001

Telephone: 1300 363 992

Fax: (02) 9284 9666

Email: enquiries@oaic.gov.auWebsite: www.oaic.gov.au**1.2 Schedule**

Entities to which this Privacy Policy relates:

- Haidnay Pty Ltd
- Kelly Engineering
- Haidnay Innovations Pty. Ltd
- Kelly Farm Management
- Haidnay Finance Co.

COMMUNICATION**QM Section: 7.4****Privacy and Notifiable Data Breaches Policy**

Notifiable Data Breaches Policy:

Kelly Engineering will take every precaution to ensure that personal information of individuals or companies are protected and stored safely in accordance with our Privacy Policy. Should we suspect that there has been a breach of your data or information, Kelly Engineering (KE) has an obligation to take appropriate remedial action.

What is an 'Eligible Data' Breach?

An eligible data breach occurs if either:

- I. there is unauthorised access to, or unauthorised disclosure of, information held by KE, or
- II. information is lost in circumstances where there is likely to be unauthorised access to or unauthorised disclosure of information; and

a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

However, if KE takes remedial action;

- a) prior to any serious harm occurring (from unauthorised access or disclosure) and, as a result of the remedial action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals;
- b) prior to any loss of information resulting in unauthorised access to or disclosure of information; or
- c) after the loss of information results in unauthorised access to or disclosure of that information, but before the access or disclosure results in any serious harm to an individual and, as a result of the remedial action, a reasonable person would conclude that the subsequent access or disclosure would not be likely to result in serious harm to the individual,

the access, disclosure, or loss (as relevant) is not, and is never taken to have been an eligible data breach.

What is 'Serious Harm'?

Serious harm may be described as serious physical, psychological, emotional, economic and financial harm as well as serious harm to reputation.

It is apparent that when assessing whether 'serious harm' is likely to occur, KE will need to apply a reasonableness test to the circumstances, in order to reach a conclusion, and those details that should be considered are as follows;

- a) the kind of information and its sensitivity;
- b) whether the information is protected by any security measures and if so, whether those security measures could be overcome;
- c) the persons or kinds of persons (Recipients) who have obtained or could obtain the information;
- d) if a security technology or methodology was used in order to make the information unintelligible or meaningless to unauthorised Recipients;

COMMUNICATION**QM Section: 7.4****Privacy and Notifiable Data Breaches Policy**

- e) the nature of the harm; and
- f) other relevant matters.

Requirement to Assess

If KE is aware that there are reasonable grounds to suspect that there may have been an eligible breach by KE but is not aware that there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach, then KE must:

- a) carry out reasonable and expeditious assessment of whether there are grounds to believe that the relevant circumstances amount to an eligible data breach of KE; and
- b) take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware of the reasonable grounds to suspect an eligible data breach.

Requirement to Notify the Commissioner of the Eligible Data Breach

As soon as KE becomes aware that there are grounds to believe that the relevant circumstances amount to an eligible data breach by them, KE must;

- a) prepare a statement that sets out;
 - I. KE's identity and contact details;
 - II. a description of the eligible breach
 - III. the types of information concerned; and
 - IV. recommendations about the steps that individuals should take in response to the eligible data breach, and
- b) give a copy of the statement to the Commissioner

The Commissioner may also direct KE to prepare a statement, if the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach.

If KE has reasonable grounds to believe that the eligible data breach was caused by another entity, the statement may also set out the identity and contact details of the other entity.

Requirement to Notify Individuals who are Harmed by the Eligible Data Breach

If KE is required to provide the Commissioner with a statement, we must as soon as practicable;

- a) take steps that are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates, if practicable; or
- b) take steps that are reasonable in the circumstances to notify the contents of the statement to each of the individuals who are at risk of the eligible data breach, if practicable; or
- c) if neither of the above apply, publish a copy of the statement on KE's website and take reasonable steps to publicise the contents of the statement.

COMMUNICATION
Privacy and Notifiable Data Breaches Policy

QM Section: 7.4***Exceptions***

If an entity prepares a statement after an eligible data breach, but that eligible data breach was caused by another entity, those other entities are not required to prepare a statement.

Documentation

All investigations of an eligible data breach and statements will be documented and filed appropriately.

References:

New notification requirements under the Privacy Act. Privacy Amendment (Notifiable Data Breaches) 2017|Mills Oakley

Privacy Amendment (Notifiable Data Breaches) Act 2017

Calvin Stead
Chief Executive Officer