1. Introduction

From time to time Neumann Steel (**the Company**") is required to collect, hold, use and/or disclose personal information relating to individuals (including, but not limited to its customers, contractors, suppliers and employees) in the performance of its business activities.

The information collected by the Company will, from time to time, be accessible to certain individuals employed or engaged by the Company who may be required to use the information in the course of their duties.

This document sets out the Company's policy in relation to the protection of personal information, as defined, under the *Privacy Act 1988* (Cth) the ("**Act**"), which includes the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)* and the Australian Privacy Principles ("**APP**"). The APPs regulate the handling of personal information.

2. Purpose

This policy outlines the Company's requirements and expectations in relation to the handling of personal information to ensure compliance to legislation and maintain the integrity of the Company's operations and the privacy of data.

3. Scope

This policy covers all employees engaged to work at the Company and all persons performing work or services at the direction of, in connection with, or on behalf of the Company. For the purposes of this policy, Employee refers to;

- Paid employees
- Volunteers
- Consultants
- Contractors
- Vocational, work experience placements and students

This policy applies in all work-related dealings with other people including colleagues, external clients, students, customers and suppliers, while in the workplace, working off-site, at work related functions and conferences, including outside ordinary business hours.

4. What is personal information?

Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

5. What is not personal information?

This policy does not apply to the collection, holding, use or disclosure of personal information that is an employee record as they are exempt from the APPs.

An employee record is a record of personal information relating to the employment of an employee. Examples of personal information relating to the employment of the employee include, but are not limited to, health information and information about the engagement, training, disciplining, resignation, termination, terms and conditions of employment of the employee.

Employees (such as those engaged in a supervisory, operations or human resource capacity) will have access to employee records. Employees who have access to employee records must ensure that the information is handled confidentially and for a proper purpose only. Employee records are only permitted to be collected, used and disclosed where the act of doing so is directly related to a current or former employment relationship.

Employees who have access to employee records and who may have a question about the use or disclosure of employee records, should contact the Human Resources Manager.

6. Types of information that the Company collects and holds

The Company collects personal information that is reasonably necessary for one or more of its functions or activities or if the Company has received consent to collect the information. If the Company collects sensitive information (as defined below), the Company must also have obtained consent in addition to the collection being reasonably necessary.

The type of information that the Company collects and holds may depend on an individual's relationship with the Company, for example:

- **Candidate:** if a person is a candidate seeking employment with the Company, the Company may collect and hold information about that candidate including the candidates name, address, email address, contact telephone number, gender, age, employment history, references, resume, medical history, emergency contact, taxation details, qualifications and payment details.
- **Customer:** if a person is a customer of the Company, the Company may collect and hold information including the customer's name, address, email address, contact telephone number, gender and age and other sensitive information.
- **Supplier:** if a person or business is a supplier of the Company, the Company may collect and hold information about the supplier including the supplier's name, address, email address, contact telephone number, business records, billing information and information about goods and services supplied by the supplier.

- **Referee:** if a person is a referee of a candidate being considered for employment by the Company, the Company may collect and hold information including the referee's name, contact details, current employment information and professional opinion of candidate.
- **Sensitive Information:** the Company will only collect sensitive information where an individual consents to the collection of the information and the information is reasonably necessary for one or more of the Company's functions or activities. Sensitive information includes, but is not limited to, information or an opinion about racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, membership of a trade union, sexual preferences, criminal record, health information or genetic information.

7. How the Company collects and holds personal information

The Company (and the employees acting on the Company's behalf) must collect personal information only by lawful and fair means.

The Company may collect personal information in a number of ways, including without limitation:

- through application forms (e.g. job applications, VIP and loyalty program applications);
- by email or other written mechanisms;
- over a telephone call;
- in person;
- through transactions;
- through the Company website;
- through lawful surveillance means such as a surveillance camera;
- by technology that is used to support communications between individuals and the Company;
- through publically available information sources (which may include telephone directories, the internet and social media sites); and
- direct marketing database providers.

When the Company collects personal information about an individual through publicly available information sources, it will manage such information in accordance with the APPs.

At or before the time or, if it is not reasonably practicable, as soon as practicable after, the Company collects personal information, the Company must take such steps as are reasonable in the circumstances to either notify the individual or otherwise ensure that the individual is made aware of the following:

- the identity and contact details of the Company;
- that the Company has collected personal information from someone other than the individual or if the individual is unaware that such information has been collected;
- that collection of personal information is required by Australian law, if it is;
- the purpose for which the Company collects the personal information;
- the consequences if the Company does not collect some or all of the personal information;
- any other third party to which the Company may disclose the personal information collected by the Company;
- the Company's privacy policy contains information about how an individual may access and seek correction of personal information held by the Company and how an individual may complain about a breach of the APPs; and
- whether the Company is likely to disclose personal information to overseas recipients, and the countries in which those recipients are likely to be located.

Unsolicited personal information is personal information that the Company receives which it did not solicit. Unless the Company determines that it could have collected the personal information in line with the APPs or the information is contained within a Commonwealth record, it must destroy the information to ensure it is de-identified unless the Company determines that it is acceptable for the Company to have collected the personal information.

8. Use and Disclosure of Personal Information

The main purposes for which the Company may use and/or disclose personal information may include but are not limited to:

- recruitment functions;
- customer service management;
- training and events;
- surveys and general research, and
- business relationship management.

The Company may also collect, hold, use and/or disclose personal information if an individual consents or if required or authorised under law.

Direct Marketing:

- the Company may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing (for example, advising a customer about new goods and/or services being offered by the Company);
- the Company may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose; and
- an individual can opt out of receiving direct marketing communications from the Company by contacting the Director in writing or if permissible accessing the Company's website and unsubscribing appropriately.

9. Disclosure of Personal Information

The Company may disclose personal information for any of the purposes for which it is was collected, as indicated under Clause 7 of this policy, or where it is under a legal duty to do so.

Disclosure will usually be internally and to related entities or to third parties such as contracted service suppliers.

If an employee discloses personal information to a third party in accordance with this policy, the employee must take steps as are reasonable in the circumstances to ensure that the third party does not breach the APPs in relation to the information.

10. Access to Personal Information

If the Company holds personal information about an individual, the individual may request access to that information by putting the request in writing and sending it to the Communications Manager or HR Manger. The Company will respond to any request within a reasonable period, and a charge may apply for giving access to the personal information where the Company incurs any unreasonable costs in providing the personal information.

There are certain circumstances in which the Company may refuse to grant an individual access to personal information. In such situations the Company will provide the individual with written notice that sets out:

- the reasons for the refusal; and
- mechanism available to you to make a complaint.

If you receive such a request, please contact the Communications Manager for any external stakeholder requests and HR Manger for internal/ employee requests.

11. Correction of Personal Information

If the Company holds personal information that is inaccurate, out-of-date, incomplete, irrelevant or misleading, it must take steps as are reasonable to correct the information.

If the Company holds personal information and an individual makes a request in writing addressed to the Communications Manager or HR Manger to correct the information, the Company must take steps as are reasonable to correct the information and the Company will respond to any request within a reasonable period.

There are certain circumstances in which the Company may refuse to correct the personal information. In such situations the Company will give the individual written notice that sets out:

- the reason for the refusal; and
- mechanism available to you to make a complaint.

If the Company corrects personal information that it has previously supplied to a third party and an individual requests the Company to notify the third party of the correction, the Company will take such steps as are reasonable to give that notification unless impracticable or unlawful to do so.

If you receive such a request, please contact the Communications Manager for any external stakeholder requests and HR Manger for internal/ employee requests.

12. Integrity and Security of Personal Information

The Company will take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that it collects is accurate, up-to-date and complete.

Employees must take steps as are reasonable in the circumstances to protect the personal information from misuse, interference, loss and from unauthorised access, modification or disclosure.

If the Company holds personal information and it no longer needs the information for any purpose for which the information may be used or disclosed and the information is not contained in any Commonwealth record and the Company is not required by law to retain the information, it will take such steps as are reasonable in the circumstances to destroy the information or to ensure it is de-identified.

If you are unsure whether to retain personal information, please contact the Communications Manager or HR Manager to discuss.

13. Data Breaches and Notifiable Data Breaches

A "**Data Breach**" occurs where personal information held by the Company is accessed by, or is disclosed to, an unauthorised person, or is lost. An example of a Data Breach may include:

- lost or stolen laptops or tablets;
- lost or stolen mobile phone devices;
- lost or stolen USB data storage devices;
- lost or stolen paper records or documents containing personal information relating to the Employer's customers or employees;

- employees mistakenly providing personal information to the wrong recipient (i.e. payroll details to wrong address);
- unauthorised access to personal information by an employee;
- employees providing confidential information to the Employer's competitors;
- credit card information lost from insecure files or stolen from garbage bins;
- where a database has been 'hacked' to illegally obtain personal information; and
- any incident or suspected incident where there is a risk that personal information may be misused or obtained without authority.

If you are aware of or reasonably suspect a Data Breach, you must report the actual or suspected Data Breach to the General Manager or relevant Department Manager as soon as reasonably practicable and not later than 24 hours after becoming aware of the actual or suspected Data Breach.

A "**Notifiable Data Breach"** occurs where there is an actual Data Breach, and:

- a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation); or
- in the case of loss (i.e. leaving an unsecure laptop containing personal information on a bus), unauthorised access or disclosure of personal information is likely to occur as a result of the Data Breach, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation).

A Notifiable Data Breach does not include a Data Breach where the Company has been successful in preventing the likely risk of serious harm by taking remedial action.

Assessment

If the Company is aware of any actual or suspected Data Breach, it will conduct a reasonable and expeditious assessment to determine if there are reasonable grounds to believe that the Data Breach is a Notifiable Data Breach or not.

Notification

Subject to any restriction under the Act, in the event that the Company is aware of a Notifiable Data Breach, the Company will, as soon as practicable, prepare a statement outlining details of the breach and notify:

- the individual whose personal information was part of the Data Breach ; and
- the Office of the Australian Information Commissioner.

14. Anonymity and Pseudonymity

Individuals have the option of not identifying them self, or using a pseudonym, when dealing with the Company in relation to a particular matter. This does not apply:

a. where the Company is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

b. where it is impracticable for the Company to deal with individuals who have not identified themselves or who have used a pseudonym.

However, in some cases if an individual does not provide the Company with the personal information when requested, the Company may not be able to respond to the request or provide you with the goods or services that you are requesting.

15. Complaints

Individuals have a right to complain about the Company's handling of personal information if the individual believes the Company has breached the APPs.

If an employee becomes aware of an individual wanting to make such a complaint to the Company, the employee should direct the individual to first contact the HR Manager in writing. Complaints will be dealt with in accordance with the Company's complaints procedure and the Company will provide a response within a reasonable period.

Individuals who are dissatisfied with the Company's response to a complaint, may refer the complaint to the Office of the Australian Information Commissioner.

16. Breach of Policy

An employee who acts in breach of this policy or any other Company policy which is referenced or related to this policy may face disciplinary action, up to and including termination of employment.

In cases where the Company has incurred costs due to an employee's breach of this policy, the Company may seek to recover such costs from the employee.

In cases where a breach of the policy involves a breach of any law, then the relevant government authorities or the police may be notified.

17. Other Policies

Employees are encouraged to read this policy in conjunction with other relevant Company policies, including:

- Social Media Policy
- Workplace Communications Policy
- Discipline and Termination Policy
- Code of Conduct Policy

18. Supporting Legislation and frameworks

Supporting legislation and frameworks relevant to this policy.

- Privacy Act 1988 (Cth)

Relevant State-based legislation may also be applicable.

19. Employee Acknowledgement

I acknowledge that I have read, understood, and agree to abide by the terms of this Policy and commit to uphold these standards.

Employee Name		Date	
Employee Signature			