AA Safety Group Ltd

Director: Tanya Andrews

Signed: *Tanya Andrews*

***Date:* 10th June 2023**

Review Date: 9th June 2024

GDPR, Confidentiality and Non-Disclosure Policy

Introduction

Our Non-Disclosure Policy sets out the company's position regarding the use of sensitive information and is adopted by all employees within the organisation. It is expected that all employees will adhere to the policy, and understand their role in handling and securing confidential, proprietary and sensitive information.

Why confidentiality is important to us

Through our operations, many employees are often given privileged access to confidential or sensitive information. This information may concern the ways within which the client's organisation functions, future plans for services or construction works, or sensitive resident and client data. In many cases it is only possible for us to work effectively with clients by internally exchanging this type of confidential or sensitive information.

We take significant steps to safeguard this information, including the following:

- all of our employees are given training on managing confidential and sensitive information
- all employees sign a confidentiality and non-disclosure agreement which ensures staff understand the need for confidentiality and the serious consequences of any breach
- We possess data security processes for obtaining, storing and disposing of confidential or sensitive data.

Security of data

We understand it is important to take steps to maintain the security of data received from our clients. All employees operate a range of IT and operational security procedures. These include:

- secure login identification for using IT systems — each time our employees access data, they are required to sign in using personalised password identification
- logical access controls — we limit access to information so that only employees needing data to be able to deliver their client work, are given access to sensitive information
- protecting our IT systems which operate behind a firewall, and use encrypted storage of data. We work with leading IT service providers, who provide state of the art security functionality
- ensuring continuous operations — we have a detailed business continuity policy in place which encompasses: secure, encrypted, data backup; offsite storage; original record handling; secure disposal
- we limit the amount of paper-based confidential or sensitive data our employees hold: any necessary confidential or sensitive paper records are kept in secure storage.

We place the following duties on all our staff.

Confidentiality

The employee shall, during their engagement with us, keep with inviolable secrecy and shall not reveal, disclose or publish to any person other than the Managing Director and the Directors or anybody named by them, any matters concerning particulars of ay project or relationship between us and our clients and shall not use for their own purposes, or for any purpose other than to effectively execute the company's obligations under the contract, any information of a confidential or sensitive nature which they may acquire or may have acquired in relation to the business or affairs between us and the client.
.
The Employee request and shall adhere to confidentiality arrangements as published and/or operated by ourselves and the client.

The Employee should report any matters regarding the vulnerability of confidential r sensitive information immediately to the Director.

Non-disclosure

Each employee signs a non-disclosure policy. A copy is included below and states:

I agree that I will hold confidentially any and all confidential and sensitive data or knowledge or information that I may obtain in the course of my employment with us.

I will keep confidential information so long as that information remains confidential and is not otherwise available in the public domain.

I will not impart the knowledge specifically acquired through this employment with us and if I at any time leave our employment. I agree not to disclose any confidential of sensitive information to any third party.