Scope

This policy applies to all of Avondale construction ltd remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Introduction and Purpose

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, Avondale Construction Limited has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

The General Data Protection Regulation 2018 requires that you appoint a Data protection officer to oversee the company compliance and act the first point of contact with company lead supervisory authority Failure to notify is a criminal offence.

The purpose is to:

- Protect Avondale construction Ltd data and infrastructure,
- Outline the protocols and guidelines that govern cyber security measures,
- Define the rules for company and personal use, and
- List the company's disciplinary process for policy violations.

Confidential Information we hold

We hold three types of information which are covered by this policy

- **Organisational information** – publicly available information about organisations and some confidential information
- **Personal information** – information about individuals such as names, addresses, job titles
- **Sensitive personal information** – in general this kind of information is only held about learners. There are, however, instances where sensitive information is held about other people. For example, information about dietary requirements at a conference might allow a person's religion to be deduced. Information about organisations is not covered by the Data Protection Act.
  However, there is sometimes ambiguity about whether certain information is personal or organisational.
- We will not hold information about individuals without their knowledge and consent.
- We will only hold information for specific purposes. We will inform data subjects what those purposes are. We will also inform them if those purposes change.

Confidential Data also Includes:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Customer leads and sales-related data.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

Access to Information

- We will seek to maintain accurate information by creating ways in which data subjects can update the information held.
- Information about Data Subjects will not be disclosed to other organisations or to individuals who are not members of our organisation, staff or trustees except in circumstances where this is a legal requirement, where there is explicit or implied consent or where information is publicly available elsewhere.
- Data Subjects have the option not to receive marketing mailings from us or other organisations. the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal datainformation:
- Data Subjects will be entitled to have access to information held about them by us and for what purpose within 40 days or submitting a request.
- Subject to any rules of the organisation awarding the funding, information will not be retained once no longer required for its stated purpose, we will not keep more than a project requires or surplus information 'just in case'. We will establish retention periods and a process to delete personal information when no longer required.
- At the beginning of this project the member of staff managing it will consult the Data Controller about any data protection implications.
- There may be situations where we work in partnership with other organisations on projects which require data sharing. We will clarify which organisation is to be the Data Controller and will ensure that the Data Controller deals correctly with any data which we have collected.

Data Security

- We have procedures for ensuring the security of all electronic personal data. Paper records containing confidential personnel data are disposed of in a secure way. Learning documents and staff records are all kept in a locked filing cabinet, IT equipment containing personal information is kept in a looked room or cupboard when not in use.
- All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep our information secure from would-be thieves. There is no point protecting the personal information we hold with a password if that password is easy to guess.
- We will make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

Device Security

Company Use.

To ensure the security of all company-issued devices and information, ACL employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters).
- Secure all relevant devices before leaving their desk.
- Obtain authorisation from the Gerry McGee operation director and/or Debbie Jonas HR Manager before removing devices from company premises.
- Refrain from sharing private passwords with co-workers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.

Personal Use.

ACL recognises that employees may be required to use personal devices to access company systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 8 characters).
- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

Email Security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, ACL requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

Transferring Data.

ACL recognises the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over ACL networks.
- Obtain the necessary authorisation from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to ACL data protection law and *confidentiality agreement.*
- Immediately alert the IT department of any breaches, malicious software, and/or scams.

Disciplinary Action.

Violation of this policy can lead to disciplinary action, up to and including termination. ACL disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.

Our Commitment

- We have a set of procedures covering all areas of our work which we follow to ensure that we achieve the aims set out above.
- We have established a business continuity/disaster recovery plan and we take regular back-ups of computer data files which are stored away from the office at a safe location.
- All new staff will be given training on the data protection policy and procedures. They will be told how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

- We will carry out an annual review of our data protection policy and procedures

The Data Protection Principles defined by the Information Commissioners Office (ICO)

Whenever collecting information about people, you agree to apply the Eight Data Protection Principles:

1. Personal data should be processed fairly and lawfully
2. Personal data should be obtained only for the purpose specified
3. Data should be adequate, relevant and not excessive for the purposes required
4. Data should be accurate and kept up to date
5. Data should not be kept for longer than is necessary for purpose
6. Data processed in accordance with the rights of data subjects under this act
7. Security: appropriate technical and organizational measures should be taken unauthorized or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the EEA unless that country or territory ensures an adequate level of data protection.

Signature:

Managing Director
Mr. Nick Curran