

## Scope

This policy applies to all of Avondale construction Limited 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, frauds, 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.

## Data Protection Officer (DPO)

In accordance with **UK GDPR, DPA 2018, and Data (use and access) Act 2025** Avondale Construction Limited has appointed **Mr Nicholas Curran Managing Director** as the **Data Protection Officer (DPO)** to:

- Oversee compliance with GDPR data protection laws.
- Function as the first point of contact for the **Information Commissioner's Office (ICO)**
- Ensure internal policies and procedures are followed.
- Failure to notify the ICO of a DPO appointment, where required, may constitute a criminal offence.

## Confidential Information we hold.

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

- **Organisational information** – public and confidential business data information
- **Personal information** – information about individuals such as names, addresses, job titles
- **Special Category Data** – in general this kind of information is employee data examples.

Health, religion, and bio metric information (when necessary).

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 collect and hold information for specific purposes.

- **Lawful basis contracts** legal obligations and legitimate interest
- **We will inform data subjects** what those purposes are acting with transparency and accountability and informing 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 modern technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

## Access to Information

- **Retention periods are defined**, and data is securely deleted when no longer needed 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.

- **We will ensure that Data Subjects** have the right to access, correct, restrict, or delete their data.
- **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.
- **Subject Access Requests (SARs)** will be responded to within one calendar month extendable under the "Stop the Clock" rule (E.G Allowing response to be paused whilst waiting for more information from employee)

## 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. Personal files contracts, company documentation are all kept securely partitioned within our cloud-based system and assigned to the individual departments with secure passwords. IT equipment containing personal information is kept in a locked 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 Construction Director** and/or Debbie Jonas HR People 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.

Avondale construction Limited 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 always protected.
- **Always use secure** and private networks.

## Email Security

Protecting email systems is a high priority as emails can lead to data theft, frauds, and carry malicious software like worms and bugs. Therefore, Avondale construction Limited 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 using company email for personal** or non – business purposes.
- **Contact and Report to the IT department** regarding any suspicious emails.

## Transferring Data.

Avondale Construction Limited recognises the security risks of transferring confidential data internally and/or externally.

To minimise 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 Avondale Construction Limited** 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 Avondale construction Limited** Data protection, UK GDPR law and [ACL confidentiality agreement](#).
- **Immediately alert the IT department** of any breaches, malicious software, and/or frauds.

## 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

Avondale construction Limited maintains the highest standard of data protection and cyber security to support this.

- We have a set of procedures covering all areas of our work to ensure compliance with **UKGDPR the Data Protection Act 2018** and the **Data (use and access) Act 2025**
- We have established a business continuity/disaster recovery plan to ensure resilience in the event of data loss, cyber incidents, or operational disruptions.
- we take regular back-ups of all critical computer data files which are securely stored off site in a protected location to prevent loss or unauthorised access computer data files which are stored away from the office at a safe location.

- All unfamiliar staff will be given training on the data protection policy and procedures. They will be told how they should store and manage personal information. Refresher training should be provided at regular intervals for existing staff.
- We will conduct an annual review of our data protection policy and procedures.

## The Data Protection Principles defined by the Information Commissioners Office (ICO) article 5.

- **1.Lawfulness Fairness and Transparency**  
Data must be processed lawfully fairly and transparently.
- **2.Purpose Limitation**  
Data must be collected for specified explicit and legitimate purposes.
- **3 Data Minimisation**  
Only data necessary for the intended purpose should be collected.
- **4.Accuracy**  
Data must be accurate and kept up to date.
- **5.Storage Limitation**  
Data should not be kept longer than necessary.
- **6. Integrity and confidentiality (Security)**  
Data must be processed securely to prevent unauthorised access or Loss.
- **7.Accountability**  
Organisations must be able to demonstrate compliance with all principles.

Signature:



**Managing Director**

Mr. Nick Curran

**Date 28/07/2025.**