

# JAMES COWIE GROUP

## DATA PROTECTION/PRIVACY POLICY

### CONTEXT AND OVERVIEW

#### Introduction

James Cowie Group including (James Cowie + Co Ltd, Hugh Logan Eng., Skerry Steel Services and The Northern Trailer Company) ("the Companies") business practices involves the gathering and using of certain information about individuals. Such information, including opinions and intentions, which relate to such individuals, is subject to certain legal safeguarding's and regulations, which are responsible for providing the parameters in which a company may utilize and process this data.

This data can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. Additionally, basic identity information such as; name, email, address, and ID numbers, web data such as location, IP address, cookies data, and RFID tags, health, genetic, and biometric data, racial or ethnic data, political opinions, and or sexual orientation, all constitute as personal data.

An organization or company which handles such data, and also one that is in such a position as to determine how to use this information, is known as a "Data Controller". As a "Data Controllers", the Companies are required to ensure their complete compliance with the requirements outlined in updated General Data Protection Regulations (GDPR). Such requirements are detailed herein this policy.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

The Companies are fully committed to ensuring the maintained and effective implementation of this policy and expects all their employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

#### Why This Policy Exists

This data protection policy ensures the Companies;

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Are open about how they store and processes individuals' data
- Protects themselves from the risks of a data breach

#### Data Protection Law

The GDPR (2018) describes how organisations, including the Companies, must collect, use, retain, transfer, disclose and destroy and personal data belonging to said organizations.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Regulation is underpinned by seven important principles. These say that personal data must:

1. Lawfulness, fairness and transparency.
2. Purpose limitation.
3. Data minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity and confidentiality (security)
7. Accountability.

## **PEOPLE, RISKS AND RESPONSIBILITIES**

### **Policy Scope**

This policy applies to:

- The head office of James Cowie Group.
- All staff of The Companies.
- All contractors, suppliers and other people working on behalf of The Companies on building/ construction sites.

It applies to all data that the Companies holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulations 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Bank details
- Next of Kin details
- Notes of disciplinary and grievance hearings
- Plus any other information relating to individuals

### **Data Protection Risks**

This policy helps to protect the Companies from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to comply with the rights of individuals under the GDPR.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

### **Responsibilities**

Everyone who works for or with or for the Companies has some responsibility for ensuring data is collected, stored and handled appropriately.

Each employee/team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring the companies meets their legal obligations.
- The management is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data the Companies holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the Companies sensitive data.
- The IT manager is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the Companies are considering using to store or process data. For instance, cloud computing services.

## **GENERAL STAFF GUIDELINES**

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

The Companies will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, strong passwords must be used and they should never be shared.

Personal data should not be disclosed to unauthorised people, either within the Companies or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees should request help from their line manager if they are unsure about any aspect of data protection.

## **DATA STORAGE**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the management.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

## **DATA USE**

Personal data is of no value to the Companies unless the businesses can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

Personal data should never be transferred outside of the European Economic Area.

Employees should not save copies of personal data to their own computers.

Always access and update the central copy of any data.

As a general rule the Companies will not send promotional or direct marketing material to another company contact through digital channels such as mobile phones, email (unless to a generic email address) or the Internet, without first obtaining their consent.

## **DATA ACCURACY**

1. The law requires the Companies to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the Companies should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- The companies will make it easy for data subjects to update the information the companies holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- 

## **SUBJECT ACCESS REQUESTS**

All individuals who are the subject of personal data held by the companies are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made to Anne Gilmurray the data controller at the companies. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 30 days, and such information shall be provided free of charge except in the case of complex or repeated requests.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

## **THE DELETION OF DATA**

All individuals have the right to have their personal data erased by the companies if:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed ;
- you are relying solely on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- You have to delete the data to comply with a legal obligation.

The erasure of personal data shall be communicated to other organisations where;

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).
- The right to erasure is not an absolute right. For example, it does not apply if processing is necessary to comply with a legal obligation, for performance of a contract or if the Companies have a legitimate interest in processing the data which is not overridden by an individual right.

## **OTHER INDIVIDUAL RIGHTS**

- Individuals have a number of other rights in relation to their personal data. They can require the Companies to:
- rectify inaccurate data
- Stop processing or erase data that is no longer necessary for the purpose of processing
- Stop processing or erase data if the individual's interests override the organisations legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data)
- Stop processing or erase data if it is unlawful
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's rights override the Companies legitimate grounds for processing data.

## **DATA BREACH**

- If the Companies (or any of them) discover that there has been a breach of HR related personal data that poses a risk to the rights and freedom of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Companies (any of them) will record all data breaches regardless of their effect.
- If the breach is likely to result in a high risk to the rights and freedom of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

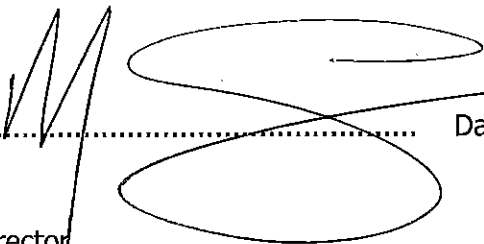
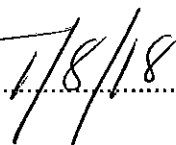
**• DISCLOSING DATA FOR OTHER REASONS**

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Companies will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

**• WHO WE SHARE DATA WITH**

We may share data with, but not limited to, our preferred Debt Collection Agencies/Field Tracing Agents and Doorstop Collection Agents to recover any unpaid debt by you to our company. This is all within our Legitimate Interests.

Signature:  Date:  .  
Mark Carney  
Managing Director