**GDPR Policy**

Context and overview

Key details

* Policy prepared by: Christine Tacey
* Approved by board/management on: 10th April 2018
* Policy became operational on: 25th May 2018
* Next review date: 10th April 2019

**Introduction**

Rood Group Limited (Roodsafe Limited, First Testing Limited & RS Safety Middle East DWC LLC) needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

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 Rood Group of Companies holds personal information for/about employees, clients and suppliers (potential and existing) under the Legitimate interests base and under the Legal obligation base where compliance with the law is necessary. Explanations of both can be found on the ICO website. Explanations of both can be found on the ICO website. We keep your information for a period of 7 years for employees or for the period of a contract for clients and/or suppliers to a maximum of 50 years.

**Why this policy exists**

This data protection policy ensures Rood Group Limited:

* Complies with data protection law and follow good practice
* Protects the rights of staff, customers and suppliers
* Is open about how it stores and processes individuals’ data
* Protects itself from the risks of a data breach

**Data protection law**

The Data Protection Act 1998 describes how organisations including Rood Group Limited must collect, handle and store personal information.

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 Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EAA), unless that country or territory also ensures an adequate level of protection

**People, risks and responsibilities**

**Policy scope**

This policy applies to:

* The head office of Rood Group Limited
* All branches of Rood Group Limited
* All staff and volunteers of Rood Group Limited
* All contractors, suppliers and other people working on behalf of Rood Group Limited

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* … plus any other information relating to individuals necessary to performing our business activitiies

**Data protection risks**

This policy helps to protect Rood Group Limited from some very real data security risks, including:

* **Breaches of confidentiality.** For instance, information being given out inappropriately
* **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

**Responsibilities**

Everyone who works for or with Rood Group Limited has some responsibility for ensuring data is collected, stored and handled appropriately. Each 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 that Rood Group Limited meets its legal obligations.
* **The Managing Director** (data protection officer) 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 Rood Group Limited holds about them (also called ‘subject access requests’).
* Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
* 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 company is considering using to store or process data. For instance, cloud computing services.
* Approving any data protection statement attached to communications such as emails and letters.
* Addressing any data protection queries from journalists or media outlets like newspapers.
* Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

**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.
* **Rood Group Limited 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 company 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 or the data protection officer 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 data protection officer.

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

Data can be erased at the subject’s request providing there is no compelling reason for its continued processing.

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 drawer or filing cabinet.**
* Employees should make sure paper and printouts are **not left where unauthorised people could see them,** like on a printer or desk.
* **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 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 devices.**
* 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 only be saved to **password protected** 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 Rood Group Limited unless the business 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:

* Personal data **should not be shared informally.**
* Data must be **encrypted before being transferred electronically.** The data protection officer can explain how to send data to authorised external contacts.
* Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

**Data accuracy**

The law requires Rood Group Limited to take reasonable steps to ensure data is kept accurate and up to date.

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.
* Rood Group Limited will make it **easy for data subjects to update the information** Rood Group Limited holds about them.
* 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 Rood Group Limited 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 by email, addressed to the data controller at info@roodsafe.com. 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.

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

The Company may make a small charge for this service.

**Disclosing data for other reasons**

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

Under these circumstances, Rood Group Limited 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.

**Providing information**

Rood Group Limited aims to ensure that individuals are aware that their data is being processed, and that they understand:

* How the data is being used
* How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

(This is available on request. A version of this statement is also available on the company’s website).