

Remote Guarding Services

Data Protection & Privacy Policy (Employee Version)

Contents

1. Introduction
2. Scope
3. Policy Statement
4. RGS – Data Protection Principles
5. Information Security
6. Responsibility for the Policy
7. Reporting of Concerns & Data Access
8. Review

1 Introduction

In order to operate efficiently and effectively we need to collect and use information about people who work for the company, such as addresses and bank details. In addition, we may on occasion be required by law to collect and use information in order to comply with the requirements of the government or in accordance with prevailing legislation. All personal information will be handled and dealt with properly however it is collected, recorded and used.

This policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.

2 Scope

This policy applies to everyone employed by RGS, including personnel working in the various divisions, from RUK to RGS Aviation.

3 Policy Statement

We regard the lawful and correct treatment of personal information as very important to the company's successful operation and to maintaining confidence between the company and our employees, we will therefore always ensure that personal information is treated lawfully and correctly and to this end we fully endorse and adhere to the Principles of Data Protection as set out in the Data Protection Act 1998.

4 RGS – Data Protection Principles

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained for only specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and where necessary kept up to date
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
7. Appropriate technical and organisational measures will be implemented to prevent unauthorised and unlawful processing of personal data and against accidental loss or destruction
8. Personal data shall not be transferred to an external organisation, unless such transference is in accordance with legislative requirements, or to facilitate the operational functioning of the company.

5 Information Security

As an employee of RGS you will have access to the company intranet and various bespoke internet-based systems, from the RGS Virtual Academy to the Site Management System. To ensure adequate safeguards are in place to protect your personal data and to facilitate the operation of the business, we will hold and process essential data about you. Such data may include (but is not limited to) your name, address, date of birth, employment history, payroll and bank details, details of illness, criminal convictions and other information as detailed in application vetting forms and employment appraisals.

This data forms part of your personnel record and will be accessible to appropriate members of staff such as Human Resources, Payroll and Operations. All data is hosted on a secure dedicated server with adequate provisions in place to ensure data security and integrity.

What information do we collect?

As a company we collect information on you:

- When you complete a vetting or application form for employment
- When you access the company intranet in order to complete specific forms such as appraisals
- Using cookies (*simple uncompiled text files that help your browser to display the full range of features offered by the company intranet*)

Who do we share data with?

We will only share your personal data with third parties if one of the following conditions is satisfied:

- You give us permission to do so
- Your employment transfers to another organisation under the Transfer of Undertakings Protection of Employment Act 2006 (TUPE)
- If we sell or buy any business or assets (in which case we may disclose certain personal data we hold to the prospective buyer or seller)
- It is necessary for the effective operation of our systems
- we are required to share your information to comply with current legislation or upon request by a government organisation (for example the police or HMRC); or
- To protect the rights, safety or property of any person.

We will not share your personal information with external organisations for marketing purposes or for economic advantage, unless a right of disclosure had been provided and appropriate consultation conducted.

6 Responsibility for the Policy

Safeguarding the integrity of employee privacy and personal data is the responsibility of company senior management, Human Resources and the designated Data Controller.

7 Reporting of Concerns & Data Access

Employees are empowered and encouraged to raise concerns if they feel their personal data has been misused in any way. Requests for access to personal data will be processed in accordance with the Data Protection Act 1998; following formal submission to the Human Resources Department and/or company designated Data Controller.

8 Review

This policy will be reviewed by the company 'Board' on an annual basis or more frequently in response to changes in legislation.

Date: 01/01/2024

Name: Waheed Javeed

Position: Director

Signature: 