EMPLOYEE PRIVACY NOTICE

Red Industries Group (RED) is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

Red is a data controller. This mean that we are responsible for deciding how we hold personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data Protection Principles
We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used fairly, lawfully and in a clear, transparent way.
2. Collected on for valid purpose that we have clearly explained to you and not used in any way that incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely, including protecting against unlawful processing, accidental loss and destruction.

Personal Information
Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

Types of personal information
We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, address, telephone numbers and personal email address.
- Date of birth.
- Gender.
- Next of kin and emergency contact information.
- Marital Status and dependents.
- Bank account details, payroll records and tax status information.
- Health screening information, including health surveillance, drug and alcohol screening.
- Employment Records, including job titles, work history, working hours, training records and professional memberships.
- Salary, annual leave, pension, and benefit information.
- Location of employment or workplace.
- National Insurance number.
- Documentation relating to your right to work in the UK, including ethnic origin.
- Driving license and insurance information (if applicable).

- Recruitment information, including CV, covering letter, references.
- Performance history, including appraisals, one to one meeting notes, files notes of discussions.
- Disciplinary and grievance information.
- Training records.
- Photographs.
- CCTV footage.
- Fingerprint scan for time and attendance system.

There are special categories of more sensitive personal data, which require a higher level of protection. We may also collect, store, and use the following 'special categories' of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Trade Union Memberships.
- Information about your health, including any medical condition, health, and sickness records.
- Information about criminal convictions and offences.

Collection of personal information
We collect personal information about employees, workers, and contractors. The initial information is collated through the application and recruitment process, either directly from candidate or sometimes from an employment agency. Further information is collated when new starter forms are completed, and other details maybe collected directly from you such as right to work documentation. We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

We operate CCTV at our sites, which records footage of individuals. Refer to our CCTV Privacy notice for more details on how this data is processed.

In some cases, we will collect data from third parties, such as employment agencies, former employees, credit reference agencies, Child Benefit agencies or other background check agencies and providers.

How will we use the personal information?
We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with legal obligation.
3. Where it is necessary for your legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
4. We may also use your personal information in the following situations, which are likely to be rare:
   a. Where we need to protect your interests (or someone else's interests).
   b. Where it is needed in the public interest (or for official purposes).

What are the situations in which we will use your personal information?
The personal information we hold on you, primarily allows RED to perform our contract with you (point 1 above). However, RED have indicated the purpose for which we are processing (or will process) your personal information, as well as indicating which categories of data are involved. The situations in which we will process your personal information are listed below:

Allows us to perform our contract with you	• Making a decision about your recruitment or appointment. • Determining the terms on which you work for us. • Providing benefits to you such as company car/cash allowance and Life Assurance. • Administering the contract, we have entered into with you.

	• Business management and planning, including accounting and auditing. • Conducting performance reviews, managing performance and determining performance requirements. • Making decisions about salary reviews and compensation. • Assessing qualifications for a particular job or task, including decisions about promotions. • Gathering evidence for a possible grievance or disciplinary hearings. • Making decision about your continued employment or engagement. • Making arrangements for the termination of our working relationship. • Education, training, and development requirements. • Managing sickness absence. • Criminal record data, only if it is appropriate for your role.
Enables us to comply with legal obligations	• Checking you are legally entitled to work in the UK. • Paying you and, if you are an employee, deducting tax and National Insurance contributions. • Liaising with your pension provider. • Dealing with legal disputes involving you, or other employees, workers or contractors, including accidents at work. • Ascertaining your fitness to work. • Complying with health and safety obligation. • To prevent fraud.
To pursue legitimate interests of our own or those of third parties provided your interests and fundamental rights do not override those interests.	• To monitor your use of our information and communication systems to ensure compliance with our IT policies. • To ensure network and information security, including preventing unauthorised access to our computer and electronic communication systems and preventing malicious software distribution. • To conduct data analytics to review and better understand employee retention and attrition rates. • Equal opportunities monitoring.

Please note, some of the above grounds for processing will overlap and there may be several grounds, which justify our use of your personal information.

If you fail to provide personal information
If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure health and safety of our workers).

Change of purpose
We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need it for another reason and that reasons are compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis, which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules where this is required or permitted by law.

Special Categories
Special categories of particularly sensitive personal information require higher levels of protections.

We need to have further justification for collecting, storing, and using this type of sensitive personal information. We have in place appropriate policy documents and internal processes depending on the type of sensitive information, which we are required to maintain when processing such data.

We may process special categories of personal information in the following circumstances:

1. With your explicit written permission.
2. Where we need to carry out legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interest) and you are not capable of giving your consent, or where you have already made the information public.

We will use sensitive personal information in the following ways:

- To comply with employment or other laws, if it relates to leaves of absence, which may include sickness absence or family related absence.
- To ensure your health and safety in the workplace, assess your fitness to work, to provide appropriate workplace adjustments to monitor and manage sickness absence and to administer benefits, if the information relates to your physical or mental health, or your disability status.
- To ensure meaningful equal opportunity monitoring and reporting, if the information relates to your race or nationality or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation.
- To comply with employment law obligations in relation to trade union membership, we will use trade union membership information to pay trade union premiums, register the status of a protected employee.

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that is it not a condition of your contract with us that you agree to any request for consent from us.

Data Sharing
We may share your data with third parties, including third party services providers and other entities in the group.

Third parties include service providers such as contractors and designed agents and other entities within our group. Third part service providers carry out the following activities:

- Payroll
- Time and Attendance platform
- Pension administration
- Benefit administration
- Printing companies for marketing purposes
- Legal / solicitors
- Occupational Health services
- Training platform
- Audit compliance
- Fulfilment of contract with customer/supplier e.g. proof of competence

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to comply with the law.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party services providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Your data will be shared with colleagues within RED where it is necessary for them to undertake their duties, such as management duties, business organisation, hosting of data.

We do not share your data with bodies outside the European Economic Area.

Data Security
Other measures are in place to protect the security of your information, which includes preventing your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. The measures include, but are not limited to:

- IT Usage Policy.
- Sharing information via secure online portals (3rd parties).
- Password protected documents.
- Training of handling personal information between parties and / or with management.
- Internal and external Audits.
- Secure storing.

Third parties will only process your personal information on our instruction and, where they have agreed to keep it secure and treat it confidentially. We limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty on confidentiality.

Internal processes are in place to deal with any suspected data security breach. Red will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention
We will retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirement. To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations. The statutory retention periods are detailed in the Personal Data Retention Schedule in Appendices A and B.

Right of access, correction, erasure and restriction
It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances, by law you have the right to:

Request access to your personal information (commonly known as a 'data subject access request').	This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
Request correction of the personal information we hold about you.	This enables you to have any incomplete or inaccurate information we hold about you corrected.
Request erasure of the personal information.	This enables you to ask us to delete or remove personal information where there is no good reason for us to continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
Object to processing of your personal information	This is where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation, which makes you want object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
Request the restriction of processing of your personal information.	This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
Request the transfer of your personal information to another party.	This enables you to share information with another company or person at your request.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party please contact the HR function in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights.). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure personal information is not disclosed to any person who has not right to receive it.

Right to withdraw consent
In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent that for that specific processing at any time. To withdraw your consent, please contact the HR function.

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to unless we have another legitimate basis for doing so in law.

Data Protection Compliance / Office
The HR function will oversee the compliance of this privacy notice.

You have the right to make a complaint at any time to the Information Commissioners Office, the UK supervisory authority for data protection issues.

Last revised: 13.06.2022

Miscellaneous
This procedure will be periodically reviewed. Any amendment to it will be notified to employees in writing by the organisation's Group HR Manager and such written advice will inform employees as to the date when any amendment comes into effect.

I have read and understand the Employee Privacy Notice.

Print Name

Signature

Date

Appendix A – Personal Data Retention Schedule

This schedule details the statutory retention periods the Company must adhere to. At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it and full authorisation from a Director to do so. Where records need to be kept for longer, consider whether they can be anonymised/ personal data removed.

Record	**Schedule last updated**	**Statutory Minimum Retention period**	**Person responsible for destruction**
Accident books, accident records, accident reports	27.05.2022	Three years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches age 21)	Sneyd, Brownhills, Walleys: Site Manager Wednesbury: Operations Manager HQ: HR Administrator
Accounting Records	27.05.2022	3 years for private companies	Group Finance Controller
COVID Job Retention Scheme	27.05.2022	6 years for furlough records	Group Finance Controller
First Aid Training	27.05.2022	6 years after employment	HR Administrators
Fire Marshall Training	27.05.2022	6 years after employment	HR Administrators
Health and Safety representatives and employees'' training	27.05.2022	5 years after employment	HR Administrators
Income Tax, NI returns, income tax records and correspondence with HMRC	27.05.2022	Not less than 3 years after the end of the financial year to which they relate.	Group Finance Controller
National Minimum wage records	27.05.2022	3 years after the end of the pay reference period following the one that the records cover	Group Finance Controller
Payroll wage/salary records	27.05.2022	6 years from the end of the tax year to which they relate.	Group Finance Controller & HR Administrators

Last revised: 13.06.2022

Record	Schedule last updated	Statutory Minimum Retention period	Person responsible for destruction
Records relating to children and young adults	27.05.2022	Until the child/young adult reaches age 21.	HR Administrators
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence (also shared parental, paternity and adoption pay records)	27.05.2022	3 years after the end of the tax year in which the maternity period ends.	Group Finance Controller & HR Administrators
Subject Access Request	27.05.2022	1 year following completion of the request.	HR Administrators
Whistleblowing documents	27.05.2022	6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately.	HR Administrators
Working time records including overtime, annual holiday, jury service, time off for dependents, etc	27.05.2022	Two years from date on which they were made.	HR Administrators

Appendix B – Other Personal Data (Suppliers, visitors, marketing etc.)

This schedule details the statutory retention periods the Company must adhere to. At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it and full authorisation from a Director to do so. Where records need to be kept for longer, consider whether they can be anonymised/ personal data removed.

Record	**Schedule last updated**	**Statutory Minimum Retention period**	**Person responsible for destruction**
Booking Forms	27.05.2022	Six years from end of last company financial year they relate to (or longer if they show a transaction that covers more than one of the company's accounting periods or the company has bought something that it expects to last more than six years, like equipment or machinery).	Group Sales Director
Complaints correspondence (relating to waste site)	27.05.2022	Until waste permit is surrendered/ revoked	?
Consignment Notes	27.05.2022	Until waste permit is surrendered/ revoked (then they must be sent to the EA).	Group Technical Operations Director
Customer/ Supplier Contracts	27.05.2022	Six years from end of last company financial year they relate to (or longer if they show a transaction that covers more than one of the company's accounting periods or the company has bought something that it expects to last more than six years, like equipment or machinery)	Group Financial Director
Customer/ Supplier Individual's Contact Information otherwise held (contact lists etc.)	27.05.2022	Once on SAP – To be updated as and when required (if person leaves company/ changes role) Other lists should subsequently be removed once on SAP, as should no longer be necessary.	Individual Departmental Managers

Last revised: 13.06.2022

Record	Schedule last updated	Statutory Minimum Retention period	Person responsible for destruction
		When lists are downloaded for manipulation/ mail shots – kept for maximum 12 months before being deleted (new lists can be generated from the system).	
Credit Account Application/ Credit Safe Report	27.05.2022	Six years from end of last company financial year they relate to (or longer if they show a transaction that covers more than one of the company's accounting periods or the company has bought something that it expects to last more than six years, like equipment or machinery	Group Financial Director
Customer Satisfaction Survey	27.05.2022	12 months after survey completed. Data retained after this to be anonymised for future analysis.	Group Marketing Manager
Databases of contacts (prospects)	27.05.2022	12 months if no contact/ interest from individual after initial contact.	Group Marketing Manager
Delivery Notes (customers)	27.05.2022	Six years from end of last company financial year they relate to (or longer if they show a transaction that covers more than one of the company's accounting periods or the company has bought something that it expects to last more than six years, like equipment or machinery)	Group Sales Director
Invoices/ Credit Notes	27.05.2022	Six years from end of last company financial year they relate to (or longer if they show a transaction that covers more than one of the company's accounting periods or the company has bought something that it expects to last more than six years, like equipment or machinery	Finance Team

Record	Schedule last updated	Statutory Minimum Retention period	Person responsible for destruction
Landfill Communities Fund Applications (Successful)	27.05.2022	Six years from date of last record.	Head of Executive Support Services
Landfill Communities Fund Applications (Unsuccessful)	27.05.2022	Two years from application decision.	Head of Executive Support Services
Orders (Customer)	27.05.2022	Six years from end of last company financial year they relate to (or longer if they show a transaction that covers more than one of the company's accounting periods or the company has bought something that it expects to last more than six years, like equipment or machinery)	Group Financial Director
Purchase Orders (Suppliers)	27.05.2022	Six years from end of last company financial year they relate to (or longer if they show a transaction that covers more than one of the company's accounting periods or the company has bought something that it expects to last more than six years, like equipment or machinery)	Group Financial Director
Quotations	27.05.2022	Unsuccessful: Two full years after rejection Successful: Six full years plus current year	Group Sales Director
Waste Carriers Licence (Suppliers/ Customers)	27.05.2022	Until superseded or expires	Transport Manager
Waste Transfer Notes	27.05.2022	Until waste permit is surrendered/ revoked.	Group Technical Operations Director

Last revised: 13.06.2022