GENERAL DATA PROTECTION REGULATIONS POLICY

RED Industries Group (RED) is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees, referred to as HR-related personal data.

This policy does not apply to the personal data of clients or other personal data processed for business purposes.

RED has appointed the HR function responsible for data protection compliance within the organisation. Questions about this policy, or requests for further information, should be directed to the HR team.

Definitions
"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles
RED Industries Group processes HR-related personal data in accordance with the following data protection principles:

- RED processes personal data lawfully, fairly and in a transparent manner.
- RED collects personal data only for specified, explicit and legitimate purposes.
- RED processes personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
- RED keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- RED keeps personal data only for the period necessary for processing.
- RED adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

RED will inform individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices.

It will not process personal data of individuals for other reasons. Where RED relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where RED processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, in accordance with the organisations Privacy Notices and Criminal Offences Policy.

RED will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems.

The periods for which RED holds HR-related personal data will be in line with the law and what is reasonably practical to manage.

RED keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights
As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests
Individuals have the right to make a *subject access request*. If an individual makes a *subject access request*, the organisation will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
- for how long their personal data is stored (or how that period is decided).
- their rights to rectification or erasure of data, or to restrict or object to processing.
- their right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

RED will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise. If the individual wants additional copies, RED will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a *subject access request*, the individual must submit a request to the HR function using RED's Subject Access Request Form. RED may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

RED will normally respond to a request within a period of one month from the date it is received. Where RED processes large amounts of the individual's data, it may respond within three months of the date the request is received. RED will write to the individual within one month of receiving the original request to tell them if this is the case.

If a *subject access request* is manifestly unfounded or excessive, RED is not obliged to comply with it. Alternatively, RED can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

A *subject access request* is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data.
- stop processing or erase data that is no longer necessary for the purposes of processing.
- stop processing or erase data if the individual's interests override the organisation's 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 processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

An individual should send the request in writing to the HR function to activate any of these steps.

Data security
RED takes the security of HR-related personal data seriously. RED has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where RED engages third parties to process personal data on its behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments
Some of the processing that RED carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches
If RED discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms 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.

International data transfers
The organisation will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities
Individuals are responsible for helping RED keep their personal data up to date. Individuals should let RED know if data held by RED requires updating, for example, address or bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, internship, or apprenticeship. Where this is the case, RED relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes.
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation.
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the data protection officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Management responsibilities
Managers (supervisors, team leaders, shift managers etc.) are accountable for ensuring employees are aware of their responsibilities in accordance with this policy. This includes educating employees on a regular basis, and ensuring new starters are aware of their obligations.

Managers are responsible for ensuring personal data (e.g., names, addresses, dates of birth, salary information, medical information etc.) shared with them directly by the employee and / or from other internal functions such as HR or Finance, is kept strictly confidential as per this policy, and must not be disclosed with anyone within the business, without prior permission from the HR function.

Managers are responsible for reporting data breaches, no matter how minor, to the HR function within 12 hours of the breach taking place. There is a legal obligation for RED to report potential data breaches to the Information Commissioners Office (ICO) if the data breach causes a likely and severe risk to the individual's rights and freedoms. The HR function will determine if such breach has occurred therefore the following information from the manager must be provided on email to the HR function to review this:

1. Description of the data breach.
2. Category / number of individuals concerned.
3. Category / number of personal data records concerned.
4. Description of the foreseeable consequences resulting from the breach.
5. Description of the measures taken, or intend to take to deal with the breach, and reverse the effects.

Training
RED will make every effort to provide training to individuals about their data protection responsibilities, as outlined in this policy. However, employees must make a reasonable effort to understand their responsibilities and query any misunderstanding or concerns about their responsibilities, with management.

Management whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them if requested.

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 General Data Protection Regulations Policy.

Print Name		**Signature**	
Date			