POLICY

Data Protection Policy

Main Author	Reviewer	Reviewer	Approver
Michel Mauricio	Liam O'Meara	Michael Carroll	Tom Barrett

REV	Date	Status / Description of Changes
01	05/08/2019	Updating all laws/regulations dates to the current standard. Adjusting template, for a more clear layout.
02	22/07/2020	Updating all laws/regulations dates to the current standard. Adjusting template, for a more clear layout.
03	07/12/2020	Minor adjustment to template
04	01/11/2021	Minor adjustment to template, laws/regulations checked

GRADEWELL
CONSTRUCTION AND PLANT HIRE

Contents

Introduction 3
The aim of this policy is: 3
Who does this apply to: 3
What is Data protection, information security and confidentiality 3
Legislation 4
Personal data an employer can keep about an employee 4
Compliance 5
Employee Rights 5
When information can be withheld 6
Disciplinary action 6
Raising a concern 6
Making a complaint 6

Introduction

We respect the privacy of our employees, clients, subcontractors and suppliers. We are fully committed to complying with all legislation regarding protection, security and confidentiality of personal data.

Personal data relates to all information (including opinions and intentions), which relates to a living individual and from which he or she can be identified and includes all medium of communicating and storing of data including but not limited to email, written on paper, stored electronically, posted, presented, spoken in conversation etc.

All staff are expected to operate in accordance with our core values and maintain high-standards in agreement with our policies and procedures.

The aim of this policy is:

1. To communicate our boards commitment and responsibilities
2. To provide an understanding of the relevant statutory, regulatory and legislative requirements

To provide clarity on our policies, procedures and expected conduct of employees and individuals

Who does this apply to:

The policy applies to anyone carrying out works for the JRL Group of companies including:

All directly employed staff whether full time or part time

Temporary contractors
Agency staff
Trainees, apprentices and work experience
Third parties that store or utilize our information

What is Data protection, information security and confidentiality

Data Protection: Is the protection of personal information held on computer systems and certain manual filing systems. The Act covers personal data held on any living individual i.e. employees, clients, subcontractors, and suppliers. Personal data means information (including opinions and intentions) which relates to a living individual and from which he or she can be identified. Such information which identifies an individual and which is being processed by computer will be personal data. The Act also applies to certain information held in manual filing systems (internally and externally structure so that specific information about a particular individual can be found easily).

Information security: Safe-guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality and integrity.

Confidentiality: The organization has an obligation to ensure that no person or organization is likely to be identified from any data released.

Legislation

We are committed to complying with data protection legislation including the General Data Protection Regulation 9EU 2016/679, coming into force on 25th May 2018 ("Data Protection Legislation") and the existing Data Protection Act 2018 (the "Act") that came into force on 1st March 2000 that regulates the capture, storage and use of information about individuals known as "Personal data".

Everyone that is responsible for using data has to follow strict rules called 'data protection principles. They must make sure the information is:

be processed fairly and lawfully

be processed for limited purposes

be adequate, relevant and not excessive be accurate

and up-to-date

not be kept for longer than is necessary

be processed in line with the rights of data subjects

be processed securely

not to be transferred to a country or territory outside the European Economic Area without adequate safeguards

There is stronger legal protection for more sensitive information such as:

Ethnic background

Political opinions

Religious beliefs

Health

Sexual health

Criminal records

Personal data an employer can keep about an employee

- Data we will keep about an employee includes:
- name
- address
- date of birth
- sex
- education and qualifications
- work experience
- National Insurance number
- tax code
- details of any known disability
- emergency contact details
- employment history with the organization
- employment terms and conditions (e.g. pay, hours of work, holidays, benefits, absence)
- any accidents connected with work any
  training taken
- any disciplinary action

Compliance

To ensure that we are achieving compliance:

Provide advice and assistance on issues arising under the Data Protection Act

Everyone handling data understands that they are responsible for following good data protection practice Queries about handling personal data are promptly dealt with

Procedures for handling personal data are clearly described
Regular risk review is made of the way personal data is managed

Authorization to obtain or disclose personal data must come from an appropriate person within our company
Provide opt in and out clauses for direct marketing material being issued to personal addresses.

Security of information is a vital part of data protection and treating information appropriately and in accordance with the risks associated with it is vital. We will:

- Ensure information will be protected from unauthorized access
- Undertake regular risk review of our hardware and software to ensure physical security of data
- Ensure confidentiality of information including any client's special security or confidentially arrangements Maintain the integrity of information
- Limit availability of information to authorized persons only
- Comply with all statutory, regulatory, legislative and contractual requirements
- Implement adequate and proportionate Business Continuity plans and regularly test and maintain these Information security training will be available to all staff

  Investigated all breaches of information security, actual or suspected, and implement mitigations to prevent these from accruing.

Every employee has an individual responsibility to ensure compliance. Unauthorized disclosure, removal or copying of personal data will be regarded as a serious disciplinary offence, and employees may also be criminally liable if they knowingly or recklessly disclose personal data without company consent.

Employee Rights

- find out what data an organization has about you

The Data Protection Act gives you the right to find out what information the organization has and stores about you and the purpose of which the date is used, or how it is intended to be used. All request for information need to be in writing to the Company Secretary and must be responded to within 40 days from the date on which the request was received. and will incur a £10 administration charge.

When information can be withheld

There are some situations when organizations are allowed to withhold information, for example if the information is about:

- the prevention, detection or investigation of a crime
- national security or the armed forces the
  assessment or collection of tax
- judicial or ministerial appointments

In these above instances, we are not obliged to say why we are withholding information.

Disciplinary action

Breaches of this policy will be regarded as misconduct and could lead to disciplinary action, up to and including dismissal / termination of contract in accordance with our Disciplinary Policy.

Raising a concern

If you suspect or have concerns that a breach of this policy has or is likely to occur, we request that you bring this to the attention of the business immediately.

In the first instance, we advise that all concerns should be directed to your line manager, if you are uncomfortable with this or if the concern is with your line manager that you can raise your issue / concern to our Company Secretary.

Making a complaint

If you think your data has been misused or that we have not kept it secure, we ask that you raise this with your line manager in the first instance or the Company Secretary.

If you are unhappy with our response or if you need any advice you can contact the Information Commissioner's Office (100).

Thomas Barrett – Director