GRADEWELL
CONSTRUCTION AND PLANT HIRE

POLICY

INTRODUCTION TO GRADEWELL POLICIES

Main Author	Reviewer	Reviewer	Approver
Michael Carroll	Liam O'Meara	Michel Mauricio	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	14/08/2020	Minor adjustment to template
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

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

Personnel data relates to all information about an individual from which that person can be identified. This includes all mediums of storing and communicating data, including written on paper, email, posted, stored electronically etc.

Gradewell Plant and Haulage Ltd expect all staff to work in accordance with the standards noted in the organisations policies and procedures.

Aim of the Policy

The aim of the policy is to communicate Gradewell Plant and Haulage Ltd commitment, obligations and responsibilities. The policy aims to provide clarity on statutory, regulatory and legislative requirements and the expected conduct of employees and individuals.

Who does this policy apply to?

The policy applies to anyone carrying out works for Gradewell Plant and Haulage Ltd. All personnel directly employed include the following:

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

Data Protection

Data protection is the protection of personnel data held on computer systems and certain manual filing systems. Personnel data means information which relates to an individual, from which the individual can be identified. The Act covers personal data held on any living individual i.e. employees, clients, subcontractors, and suppliers.

Information security

Information security is the safe-guarding of an organisation's data from unauthorised access or modification to ensure its availability, confidentiality and integrity. The organisation has an obligation to ensure that no person or organisation 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 25th May 2018 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 organisation
- employment terms and conditions (e.g. pay, hours of work, holidays, benefits, absence)
- any accidents connected with work any training taken
- any disciplinary action

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
- Authorisation 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 unauthorised 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 authorised 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. Unauthorised 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 organisation has about you

The Data Protection Act gives you the right to find out what information the organisation has and stores about you and the purpose of which the date is used, or how it is intended to be used. All requests 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 organisations 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 manager.

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 manager.

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

Michael Carroll – Complaint Manager

Thomas Barrett – Director