Greenfield engineering

T: +44 (0)1409 254400
F: +44 (0)1409 254898
enquiries@greenfieldengineering.co.uk
GREENFIELDENGINEERING.CO.UK

DATA PROTECTION POLICY

INTRODUCTION

Greenfield Engineering needs to gather and use certain information about individuals.

This can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

WHY THIS POLICY EXISTS

This data protection policy ensures Greenfield Engineering

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and suppliers
- Is open about how it stores and processes individuals data
- Protects itself from the risk of a data breach

DATA PROTECTION LAW

The Data Protection Act 1998 describes how organisations, such as Greenfield Engineering, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

T: +44 (0)1409 254400 enquiries@greenfieldengineering.co.uk
F: +44 (0)1409 254898 **GREENFIELDENGINEERING.CO.UK**

PEOPLE, RISKS AND RESPONSIBILITIES

POLICY SCOPE

This policy applies to:

- Greenfield Engineering Neet Way Site
- Greenfield Engineering Waldon Way Site
- All Staff of Greenfield Engineering

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone Numbers (incl mobile no:)
- Dates of birth
- Next of kin details
- Payment information incl. Bank details
- ….plus any other information relating to individuals

DATA PROTECTION RISKS

This policy helps to protect Greenfield Engineering from some very real data security risks,

Including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

T: +44 (0)1409 254400 enquiries@greenfieldengineering.co.uk
F: +44 (0)1409 254898 **GREENFIELDENGINEERING.CO.UK**

RESPONSIBILITIES

Everyone who works for or with Greenfield Engineering has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Greenfield Engineering meets its legal obligations.
- The Data Protection Officer, Kerris Pass is responsible for:
- Keeping people updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies.
- Arranging data protection training and advice for people covered by this policy.
- Handling data protection questions from staff and anyone covered by this policy.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Maintain an ongoing commitment to reviewing systems, processes and procedures and updating if necessary to ensure data is stored and managed in a secure manner.
- The Material Planning & Operation Manager, Daniel Green, is overall responsible for:
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Dealing with requests from individuals to see the data Greenfield Engineering holds about them (also 'subject access requests')
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspaper and radio broadcasting companies.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

GENERAL STAFF GUIDLINES

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their managers.
- Greenfield Engineering will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared. Protocols have been placed to ensure passwords must be strong and changed regularly.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their manager or the data protection officer if they are unsure about any aspect of data protection.
- A responsible and common sense based approach must be adopted by all staff to ensure data is handled in the correct manner on a day to day basis.
- Greenfield Engineering will securely hold all personnel data for an agreed period of time as requested by our insurers.

T: +44 (0)1409 254400 enquiries@greenfieldengineering.co.uk
F: +44 (0)1409 254898 **GREENFIELDENGINEERING.CO.UK**

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Material Planning and Operations Manager.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see or access it. When data is no longer required it must be shredded immediately and securely.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be securely stored.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or desk.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees or unauthorised personnel.
- If data is stored on removable media (like a HDD or USB), these should be stored securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

DATA USE

Personal data is of no value to Greenfield Engineering unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be transferred securely. The Material Planning and Operations Manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

T: +44 (0)1409 254400 enquiries@greenfieldengineering.co.uk
F: +44 (0)1409 254898 **GREENFIELDENGINEERING.CO.UK**

DATA ACCURACY

The law requires Greenfield Engineering to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Greenfield Engineering should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a supplier's/customer's details when purchase orders are received or raised.
- Greenfield Engineering will make it easy for data subjects to update the information Greenfield Engineering holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if an employee can no longer be reached on their stored telephone number, it should be removed from the database.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by Greenfield Engineering are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.
- Request for their personal data to be permanently deleted.

If an individual contacts the company requesting this information, this is called a subject access request. If an individual requests for the personal data to be permanently deleted this is known as right to erasure

'Subject access requests' and 'right to erasure' from individuals should be made by either email to kerris@greenfieldengineering.co.uk or via contact by phone or in person. 'Subject Access request' and 'Right to Erasure' forms are available on Greenfield Engineering's intranet site and a hard copy will be supplied to any individual requesting this information.

In order to fulfil these requests and before handing over or permanently deleting any personal data, Greenfield Engineering will need to verify the identity of anyone making these requests by requesting original photographic identification and a completed form. Once completed these request forms will be stored in a secure location for 7 years before being destroyed.

In accordance with GDPR Legislation, there is no fee for this request, and the data controller will provide the relevant data within 31 days of the request being made.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, Greenfield Engineering will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Greenfield engineering

T: +44 (0)1409 254400
F: +44 (0)1409 254898
enquiries@greenfieldengineering.co.uk
GREENFIELDENGINEERING.CO.UK

PROVIDING INFORMATION

Greenfield Engineering aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy policy, setting out how data relating to individuals is used by the company.