Data Protection Policy

This part of our handbook sets out a brief summary of how we handle personal data and the rules you must follow when you handle personal data in the course of your duties.

For full details of our rules and procedures on data protection and the legal conditions provided by the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA) about the obtaining, handling, processing, storage, transportation, and destruction of personal information please refer to our Privacy Standard.

For further details about the personal data we process about our staff and your rights in relation to that data, please refer to the Employee Privacy Notice.

This policy does not form part of any employee's contract of employment, and we may amend it at any time.

Definition of data protection terms

"Data subjects" for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

“Personal data” means information which relates to a living person who can be identified from that data (a ‘data subject’) on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data

"Data controllers" are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with GDPR. We are the data controller of all personal data used in our business.

"Data processors" include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

“Processing” means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

"Special categories of personal data” are types of personal data consisting of information as to:

- your racial or ethnic origin;

- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

Data protection principles

Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant. For full details of how we apply these principles, please refer to our Privacy Standard.

Dealing with subject access requests

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately to Claire Trundle, Head of HR & Administration, who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to Claire Trundle. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact Claire Trundle immediately and keep any evidence, you have in relation to the breach.

How should you process personal data for the Company?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Privacy Standard.

The Directors are responsible for reviewing this policy and maintaining compliance with the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to Claire Trundle.

- You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Personal data should be encrypted before being transferred electronically to authorised external contacts.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and with authorisation from a Director.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from Company's premises or off site without authorisation from a Director.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from Claire Trundle if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Refer to Claire Trundle or to a Director for assistance in difficult situations.

Breaches of this policy

If you consider that this policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager.

Any breach of this policy will be taken seriously and may result in disciplinary action.

Stuart Read
Executive Chairman
Readie Construction Ltd.
01st June 2022
*This policy statement is subject to annual review. It will only be published when materials changes occur.