GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

Air 3 policy principles

The Company ("Data Controller") takes the security and privacy of your data seriously. The Company needs to gather and use information or 'data' about you as part of our business and to manage our relationship with you. The Company shall comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security.

Air 3 complies with the data protection principles set out below. When processing personal data, we will endeavour to:

1. process all information lawfully, fairly and in a transparent manner in relation to the data subject
2. collect and process only the data or information which is needed
3. use personal data for such purposes as are described at the point of collection, or for purposes which are legally permitted
4. strive to ensure information is accurate
5. keep information for only as long as is necessary
6. securely destroy data which is no longer needed
7. take appropriate technical and organisational security measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data)

Air 3 will ensure that the rights of people about whom information is held can be fully exercised under the General Data Protection Regulation and facilitate any request from someone who wishes to exercise their rights under data protection law as appropriate without undue delay.

'Data Protection Law' includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation.

These rights include:

- The right to be informed
- The right of access to personal information
- The right to request rectification
- The right to request erasure
- The right to restrict processing in certain circumstances
- The right to data portability
- The right to object to processing

Information sharing

We may need to pass relevant information about you to other people and organisations or where we have an information sharing agreement to deliver a service. These people and organisations are obliged to keep your details securely, and use them only in accordance with data protection legislation so you can be confident they all comply with the same privacy principles.

We may disclose information when necessary to prevent risk of harm to yourself or another individual.

At no time will your information be passed to organisations for marketing or sales.

Privacy Policy

We are committed to safeguarding the privacy of employee and professional contacts.

In terms of employees the information we hold are personal details such as:

- Personal details, including name, title, address, telephone number, personal email address, date of

birth, gender, employment history, qualifications;

- Professional/ Occupational Qualifications;
- Next of kin details and emergency contact information;
- Disciplinary cards; and
- Information about your right to work in the United Kingdom

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your health, including any medical condition, health and sickness record;
- Drug and alcohol results data, if appropriate; and
- Information about criminal convictions and offences (if relevant to the contract you are working on).

In terms of professional contact information such as telephone and email will be needed but no further information should be required by the Company.

No information will be passed to anyone outside of head office and will be held securely on our electronic system accessible only to head office staff.

Data Breach

The Company has a process 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 the Company will document and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then the Company must also notify the Information Commissioner's Office within 72 hours.

Please note, third parties are not used to process personal data minimising the risk of any data breach.

Peter Morgan

Managing Director