ASCENT FLIGHT TRAINING (MANAGEMENT) LIMITED PRIVACY STATEMENT

Ascent Flight Training (Holdings) ("we", "us", "our", or "Ascent") are committed to ensuring that the UK General Data Protection Regulations ('UK GDPR') are observed and compliance is maintained at all times. This Notice ensures that where necessary any person can view Ascent's fulfilment of the intentions of the UK GDPR, and the key principles to which it refers. We are committed to ensuring, via the use of our Data Protection Policy, and other privacy notices we may give you in specific circumstances (including for recruitment purposes), that we explain clearly at all times how we will collect, store and use your personal data.

1. INTRODUCTION

This Privacy Statement sets out how Ascent handle the personal data of our customers, suppliers, employees, workers and other third parties including those of the military community with whom we share our partnership or otherwise.

This Privacy Statement applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject.

We may update this Privacy Statement from time to time depending on the development of the legislation or any related legislation, and we will ensure that this becomes available to be viewed on our website. For the purposes of this Privacy Statement, we refer to the UK General Data Protection Regulation (UK GDPR), under Part 2 of the Data Protection Act 2018 (DPA 2018), or any supplementing legislation.

Please take the time to read this Privacy Statement to ensure that you understand how we may process your personal data.

2. SCOPE

We recognise that the correct and lawful treatment of personal data will maintain confidence in Ascent and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.

Ascent is exposed to potential fines of up to approximately £18 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

All responsible parties, including employees, senior management and directorship of Ascent, are responsible for ensuring all Ascent personnel comply with this Privacy Statement and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Data Protection Officer ('DPO') is responsible for overseeing this Privacy Statement and, as applicable, developing related policies and privacy guidelines. Our nominated DPO can be contacted using the address below:

Email: DPO@ascentflighttraining.com

3. INFORMATION WE MAY COLLECT

We may collect and process information about you through various means, including:

- In the course of carrying out any business with you
- Via the use of our website, including any job applications submitted
- By email
- By telephone or fax
- By other non-electronic means such as business card exchange or networking events
- Via the use of security at any of our sites, for example the use of CCTV
- Otherwise via any other means

We may collect, store, and use the following personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Performance information.
- Disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Photographs.
- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

Each time you visit our website, we may automatically collect the following information:

- Any web usage information (including IP addresses), browser types, or time zones

Where we hold any discussion with you via any medium, including telephone or email, we may keep a record of that correspondence.

4. HOW WE WILL USE THE INFORMATION YOU PROVIDE

We may use your information for the following purposes:

- For any reason allowed by law
- To manage our relationship with you, including the completion of contractual obligations or other obligations pursuant to any terms of business that we have with you
- To ensure that we are fully compliant with any related legislation including but not limited to carrying out anti-money laundering checks in line with obligations imposed by our banks, anti-bribery or Modern Slavery checks
- To process any job application submitted by you or by any person on your behalf
- Where it is pursuant to any other legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests
- To prevent any illegality as we feel is necessary.

5. GDPR PRINCIPLES

We ensure that we adhere, and are accountable, to the principles relating to the processing of personal data set out in the UK GDPR which requires your personal data to be:

- Processed lawfully, fairly and in a transparent manner
- Collected only for specific, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and where necessary kept up to date
- Not kept in a form which permits identification of any subject of any data for longer than is necessary for the purposes for which the data is processed
- Processed in a secure manner
- Not transferred to another country without appropriate safeguards in place
- Made available to you upon request subject to any Data Subject Request.

6. LEGAL BASIS FOR COLLECTING DATA

We rely on the following principles outlined in the UK GDPR to allow for data processing in specific purposes:

- Performance of, or entry into, a contract (for example an employment contract with you)
- Compliance with any legal obligation to which we are subject
- Where it is pursuant to any other legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests

7. YOUR RIGHTS

The UK GDPR, and other data protection legislation, gives you the right to access any information we hold about you. You are entitled, where applicable by law, to:

- **Request access** to your personal information (commonly known as a 'data subject access request') – this enables you to receive a copy of the information we hold about you, and to check that we are processing it lawfully
- **Request correction** of the personal information that we hold about you – this enables you to have any incomplete or inaccurate information we hold about you corrected
- **Request erasure** of your personal information – this enables you to ask us to delete or remove personal information where there is no good reason for us to continue processing it
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party)
- **Request the restriction of processing** of your personal information – this enables you to ask us to suspend the processing of personal information about you
- **Request the transfer** of your personal information to another party.

You will not have to pay a fee to access your personal information (or to exercise any of your other rights above). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive.

8. SENDING INFORMATION OUTSIDE OF THE EEA

If we need to share your personal data with any recipient outside of the European Economic Area ("EEA") (e.g. for the purposes of professional services, or training), we will ensure that this is conducted in compliance with the UK GDPR or related data protection legislation.

Our personnel are occasionally permitted to access our systems when working remotely and abroad, including from jurisdictions outside the EEA. Where this occurs, they will be required to use our systems and access any personal data in accordance with our data protection policies, procedures and statements.

9. COMPLAINTS AND INFORMATION

If you wish to contact us for any reason regarding the use of your personal data, please contact our DPO at the contact details in section 2.

You also have the right to make a complaint to the Information Commissioner's Office should you wish. For more information, please visit the ICO website at:

https://ico.org.uk/concerns/handling/