DATA PROTECTION POLICY

CREATED: MAR 2018

REVISION:

APPROVED BY THE BOARD: MAY 2018

This policy relates to the Westminster Group Plc and its subsidiaries:

Westminster International Ltd

Westminster Aviation Security Services Ltd

Longmoor Security Ltd

DATA PROTECTION POLICY

POLICY SCOPE

The Westminster Group Plc and its subsidiary companies (Group) are registered under the Data Protection Act.

The Group is required to process relevant personal data regarding employees, suppliers, customers, agents and other business partners as part of its operation and will take all reasonable steps to do so in accordance with this Policy.

This policy applies to the processing of Personal Information by any employees or suppliers of the Westminster Group Plc or its subsidiaries.

THE PRINCIPLES

The Group shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:-

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Kept secure
- Not transferred to other countries without adequate reason or protection

RESPONSIBILITIES

The Group has given the Group Operations Director the responsibility for Data Protection within the Group. The Group Operations Director will endeavour to ensure that all personal data is stored and processed in compliance with this Policy, the Principles of the Data Protection Act 1998, the EU General Data Protection Regulation EU 2016/679 (GDPR) and any additional local legislation.

The Group Operations Director can be contacted on +44 1295 756300 or info@wg-plc.com.

Staff Responsibilities

Staff members who process personal data about staff, customer, business partners or any other individual must comply with the requirements of this policy.

Staff members must ensure that:

- all personal data is kept securely
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party

- personal data is kept in accordance with the Group's Data Retention Policy
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Group Operations Director
- any data protection breaches are swiftly brought to the attention of the Group Operations Director and provide any support required in resolving breaches
- where there is uncertainty around a Data Protection matter advice is sought from the Group Operations Director

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Group Operations Director.

Third-Party Data Processors

Where external companies are used to process personal data on behalf of the Group, responsibility for the security and appropriate use of that data remains with the Group.

Where a third-party data processor is used:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data
- reasonable steps must be taken to ensure that such security measures are in place
- a written contract establishing what personal data will be processed and for what purpose must be set out

For further guidance about the use of third-party data processors please contact the Group Operations Director.

PERSONAL DATA

Personal data means any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personal data covers both facts and opinions about an individual where that data identifies the Data Subject.

PROCESSING OF PERSONAL DATA

Consent may be required for the processing of personal data unless processing is necessary for the performance of a contract such as a contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.

The Group from time to time processes some personal data for direct marketing and other business purposes, Data Subjects are required to opt-in to these activities, and may opt-out again at any time.

The Data Subjects choice will always be respected.

SENSITIVE PERSONAL DATA

The Group may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings.

RIGHTS OF ACCESS TO INFORMATION

Data Subjects have the right of access to information held by the Group, subject to the provisions of the Data Protection Act 1998. Any Data Subject wishing to access their personal data should put their request in writing to the DPC. The Group will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days. The information will be imparted to the data subject as soon as is reasonably possible after it has come to the Group's attention and in compliance with the relevant Acts.

EXEMPTIONS

Certain data is exempted from the provisions of the Data Protection Act which includes the following:-

- National security and the prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Group.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the Group Operations Director.

ACCURACY

The Group will endeavour to ensure that all personal data held in relation to all Data Subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data Subjects have the right to have any personal data held that is inaccurate or incomplete rectified, this does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply. In certain circumstances, where data is no longer required by the company, for the fulfilment of a contract for example, Data Subjects can also the Group to erase or restrict the use of any personal data that we process.

ENFORCEMENT

If an individual believes that the Group has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the Data Subject should notify the Group Operations Director.

DATA SECURITY

The Group will take appropriate technical and organisational steps to ensure the security of personal data.

All staff will be made aware of this policy and their duties under the Act.

The Group and all employees, agents and other business partners are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be encrypted when transported offsite.

Attention is also drawn to the existence of the Company IT & Security Policy, which provides more specific information on digital data security measures which should be taken, and best practice guidelines.

EXTERNAL PROCESSORS

The Group will ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant legislation.

SECURE DESTRUCTION

When data held in accordance with this policy is destroyed, it will be destroyed securely in accordance with best practice at the time of destruction.

RETENTION OF DATA

The Group may retain data for differing periods of time for different purposes as required by statute or best practices, individual departments should incorporate these retention times into the processes and manuals. Other statutory obligations, legal processes and enquiries may also necessitate the retention of certain data.

The Group may store some data such as photographs, testimonials and project notes indefinitely in its marketing materials.

The Group has a general data retention period of 6 years during which time data may reside on backup media before final destruction.

CCTV

The Group owns and operates multiple CCTV systems, both in its own premises and within that of customers, for the purposes of public safety and crime prevention.

Automated Number Plate Recognition (ANPR) cameras are operated for automated vehicle access in places.

Where a data subject can be identified, images must be processed as personal data.

DATA PROTECTION BREACHES

Where a Data Protection breach occurs, or is suspected, it should reported immediately to the Group Operations Director as the primary point of contact and Where the suspected breach is IT related the IT Team as a secondary point of contact. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.

A record of any Data Breach will be maintained by the Group Operations Director.

Action may be taken against any party which has wilfully or negligently caused a Data Breach.

Peter Fowler
Chief Executive Officer

Westminster Group Plc