



DATA PROTECTION POLICY

1. STATEMENT OF PURPOSE AND SCOPE

- 1.1. The Company is required to hold for business and legal reasons a variety of information relating to individuals, including its employees. The type of information held includes personal details, sickness and attendance records, disciplinary records, and other information.
- 1.2. In collecting, holding and using any such data, the Company wants to ensure that it complies both with the law and with best practice and that all data which it holds in relation to its employees is relevant to their employment, complete, accurate and up-to-date, and remains confidential.
- 1.3. The Company aims to fulfil its obligations under the Data Protection Act 1998 to the fullest extent.
- 1.4. This Policy applies to all employees of the Company and relates to all forms of Personal Data and Sensitive Personal Data held by the Company, whether held on computer, paper or any other medium.

2. DATA PROTECTION

- 2.1. "Personal Data" means any data which relates to an individual and from which (or from the data and other information available or likely to be available to the Company) that individual can be identified.
- 2.2. "Sensitive Personal Data" means personal data consisting of information as to the individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership (or non-membership) of a trade union, physical or mental health or condition, sexual life, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.
- 2.3. There are circumstances where it is necessary for the Company or any Group Company, for the purpose of an employee's employment, or for compliance with any contractual, statutory, management or other similar obligations, to hold, collect or otherwise process Personal Data relating to its employees and/or their employment. It is permissible for the Company to process and disclose to third parties Personal Data provided it complies with certain legal principles set out in the Data Protection Act. The Company may also process Sensitive Personal Data which relates to any employee provided it

THE LIBERTY INTERNATIONAL GROUP – DATA PROTECTION POLICY



DATA PROTECTION POLICY

complies with certain legal principles relating to such Data. It may from time to time be necessary for the Company to obtain consent from employees to the processing of Sensitive Personal Data which relates to them.

3. PERSONAL DATA CONCERNING YOU

- 3.1. Employees are entitled to have access to all Personal Data and Sensitive Personal Data held about them under the Data Protection Act. This Act requires the Company to respond to your request for access to personal data within 40 days of a request.
- 3.2. Employees are entitled to have any Data held in relation to them corrected if that information is inaccurate. In order to ensure that all Personal Data and Sensitive Data is up to date and accurate, employees should inform the Personnel Department of any changes to their Personal Data, such as name, address, marital status, contact details, qualifications and next of kin, etc. Employees should inform the Data Protection Officer at the earliest opportunity if they believe that any of their Personal Data is inaccurate or untrue, or if they are dissatisfied with the information in any way.
- 3.3. In the event of a disagreement between an employee and the Company regarding the processing or accuracy of any Personal Data, the matter should be taken up under the Company's formal grievance procedure.

4. YOUR RESPONSIBILITIES AS AN EMPLOYEE

- 4.1 The Company will take all reasonably practicable steps to ensure that any employee who has access to, uses or otherwise processes Personal Data is appropriately trained and, where relevant, supervised to do so. If your job includes processing of Personal Data, ensure you receive appropriate training regarding Data Protection.
- 4.2 Employees must not (and must use their best endeavours to ensure that any third party acting on behalf of the Company does not) obtain, use, disclose, transfer or procure the transfer, use or disclosure of or otherwise process any employee's Personal Data or Sensitive Personal Data other than in the normal course of their duties without the prior written authorisation of the Data Protection Officer. Any employee who obtains, uses, processes or has access to any other employee's Personal Data or Sensitive Personal Data is required to keep that Data secure from unauthorised access, disclosure, use, accidental loss, damage or destruction.



DATA PROTECTION POLICY

- 4.3 Employees should inform the Data Protection Officer if they become aware of any breach of the Data Protection Act 1998.
- 4.4 Breach of this Policy and any associated rules could result in disciplinary action (including, where appropriate, dismissal) and may constitute a criminal offence.

All queries concerning this policy should be addressed to The Data Protection Officer in the first instance.

The Data Protection Officer for the Company is John Armstrong, Assistant Company Secretary. Tel: 0207 887 7064.