F.S. Mackenzie Ltd - Data Protection Policy

(*Data Protection Act 2017*)

With effect from May 2018, the Company works strictly within the guidelines and requirements of the Data Protection Act 2017 (the "Act") (previously the Data Protection Act 1998). We take our responsibilities seriously by treating all personnel/private data in a secure way and any such data provided during your employment, will only be processed for legitimate business reasons and for the purposes of your employment with the Company as additionally advised to you upon signing your contract of employment. You will also be required to give your specific and explicit consent (opt-in) for this processing to take place within the remit of the Act.

Sensitive information provided such as sickness or health records, ethnic monitoring or trade union membership details will be treated as sensitive information and will not be disclosed unless they directly affect your employment. In the event of such disclosure, only your manager, our internal HR team or external providers (PSM HR Outsourcing) and members of the senior management team directly involved in your employment, will have restricted access. Processing may involve the monitoring of various Company policies in line with good employment practice and statutory requirements.

During the course of your employment, you will have access to or be required to process and/or authorise the processing of personal/private data relating to employees, customers and other individuals held and controlled by the Company. You agree to comply with the terms of the Act as amended from time to time. The company will normally retain employee records/data for at least 6 years after an employee's termination of employment so as to facilitate post-employment referencing requests. All data will be securely erased or destroyed as and when it is appropriate.

The Act's provisions, also cover both personal and company phones (including any text messages), personal and company laptops/computers and any other postings on personal social networking websites. Whilst appropriate and authorised access and retention is acceptable for company equipment or personal equipment used for legitimate company use, it is company policy that no company information/documents etc should be permanently "retained" on any personal devices. Any employee who stores or without proper legitimacy seeks to process any data on their personal devices, will be subject to the Company's Disciplinary procedure and such conduct, could result in dismissal.

Why the Company Need to Retain Personal Data
Employees should be aware that it is essential for personal data to be retained by the Company, as otherwise, HR software systems including the booking and management of annual holiday's/absence, payroll administration, pension management or other employee related benefits and processes cannot be administered by the Company.

Access to your Personal Data/Records
If you wish to verify that the personal data that the Company holds about you is accurate, you are entitled, under the Act, to make a "Subject Access Request (SAR)" in order to see information held on your manual personnel file, on any relevant computerised/electronic systems or data base and any other company documents. Your SAR should be made to HR or a member of senior management in writing and they will arrange for you to see the relevant personnel records/information within 1 month of your request. The company can refuse a request or make a charge for requests that are manifestly unfounded, complex or considered as unreasonably excessive. However you have the right to complain to senior management if any request is refused on the basis of being excessive or unreasonable on your part and any such complaint must be made without undue delay and at the latest within one month of a refusal.

If you disagree with any information/data held on you or if you find what you view as factually incorrect data in your records, you are entitled to request that HR or a member of senior management review the accuracy of the data. If you deem it to be appropriate, you can request HR or senior management to correct or erase the data. Should it be concluded that the information is incorrect or unnecessary, then they will arrange to correct or to delete the inaccurate information as quickly as operationally possible. Although an employee has the right to erase data (also known as "the right to be forgotten") it is not an absolute right, as if it is concluded that the data is accurate and necessary for the company's requirements (e.g. processing payroll) then your request can be refused. However you are entitled to submit a formal grievance under the Company's grievance procedure.

The Act requires that any personal data held should be:

- processed fairly and lawfully in accordance with data protection principles
- obtained and processed only for specified and legitimate purposes
- adequate, relevant and not excessive
- accurate and kept up to date by regular reviews/audits
- held securely and for no longer than is necessary

Purposes for which Personal Data may be held

Personal data relating to employees may be collected legitimately/primarily for the purposes of:

- recruitment, promotion, training, redeployment and for career development
- administration and processing of payroll for the payment of salaries
- administration of HR including the use of an external HR Outsourcing Company
- Company IT systems including breatheHR system
- calculation of certain benefits including pensions
- disciplinary or performance management purposes
- performance reviews
- recording of communication with employees and their representatives
- compliance with legislation and in accordance with regulatory authorities
- provision of references to organisations, for example to facilitate entry onto educational courses and/or to assist future potential employers
- disclosure and barring service (DBS) administration
- employee structure and career planning.

The Company considers that the following personal data falls within the categories set out above:

- personal details including name, address, age, status and qualifications
- where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant
- references and CVs
- emergency contact details
- notes on discussions between management and the employee
- appraisals and documents, relating to grievance, discipline, promotion, demotion or termination of employment
- training records
- salary, benefits and bank/building society details
- absence and sickness information.

Upon receipt of a written request from employees, potential employees or ex-employees, they will be advised by the Company of the personal data which has been obtained, retained and were necessary to enable the organisation to conduct one or more of the “purposes” detailed in this policy. The Company will review the nature of the information being collected and held, generally every two years, so as to ensure there are sound and legitimate business reasons for requiring the information to be obtained and retained.

Sensitive Personal Data

Sensitive personal data (known as “special categories of personal data”) includes information relating to the following matters:

- the employee’s racial or ethnic origin
- their political opinions
- their religious or similar beliefs
- their trade union membership
- their physical or mental health or condition
- criminal convictions and offences committed by the employee.

The employee’s explicit written consent for the collection and processing of all personal data, is required by signing the declaration at the end of this policy or by the specific electronic statement that you have read, understood and unconditionally accept the terms of this policy.

Lawful Basis for Processing

In accordance with Article 6 of the General Data Protection Regulation (Act), the Company’s basis for processing of personal data will be “Consent”, whereby it is deemed that individuals have given clear

consent for the Company and/or PSM HR Outsourcing on their behalf, to process their personal HR data.

Responsibility for the Processing of Personal Data
The Company has appointed a Data Protection Officer (Controller) as the named individual responsible for ensuring all personal data is controlled in compliance with the Act. Any data breaches will be investigated and reported by this person to the Information Commissioner's Office (ICO) as necessary.

Employees who have access to personal data must comply with this policy and adhere to the procedures laid down by the Data Protection Officer and failure to comply with the policy and procedures may result in disciplinary action up to and including summary dismissal.

Use of Personal Data
To ensure compliance with the Act and in the interests of privacy, employee confidence and good employee relations, the disclosure and use of information held by the Company is governed by the following conditions:

- personal data must only be used for one or more of the purposes specified in this policy
- where any company document includes a statement of its intended use, the documents will only be used in accordance with any such use
- provided that the identification of individual employees is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data (e.g., surveys, staffing level figures)
- personal data must not be disclosed, either within or outside the Company, to any unauthorised recipient.

Personal Data Held for Equal Opportunities Monitoring Purposes
Where personal data obtained about candidates is to be held for the purpose of Equal Opportunities monitoring, all such data must be made anonymous.

Disclosure/Sharing of Personal Data
Personal data may only be disclosed outside the Company for legitimate business reasons and for the purposes of your employment with the Company and personal data will only be processed and shared with third parties for legitimate and appropriate business reasons. This can include, but is not limited to the processing of our payroll; sending appropriate data to our insurance companies that provide various employee insurance related benefits; sharing the data with PSM HR Outsourcing, who are the HR advisory company that manages the HR database, breatheHR; our IT company who maintain the Company's IT systems and dealing with requests from any regulatory bodies such as HMRC.

Introduction/Design of a New IT system
The Company will ensure that when any major new changes are being considered in relation to any employee related IT systems, data protection and security is a core element in the design of any new systems, and it will adopt a "privacy by design" approach from the onset as a key part of this process. This will ensure that when data processing is a high risk, the company will ensure from the onset that these risks are identified and suitable data protection controls implemented and linked to company processes such as risk and project management.

Accuracy of Personal Data
The Company will conduct reviews of personal data to ensure that it is accurate, relevant and up to date. In order to ensure these standards are maintained and so that the Company is able to contact the employee or, in the case of an emergency, another designated person, employees must notify the Company as soon as possible of any change in their personal details (e.g. change of name; address; telephone number; loss of driving licence where relevant; next of kin details; etc).

Employees will be entitled to update their own details where systems exist enabling them to do so or to ask for the Company to amend any incorrect details and these corrections will be made to all files/records held on the Company's information or data base systems. In some cases, documentary evidence, e.g., qualification certificates, may be requested before any changes are made. Once completed, these records will be stored in the employee's personnel file or held on any automated HR recording systems.

Declaration and Consent

I have read, understood and unconditionally accept the Company's Data Protection Policy authorising my personal data to be held and processed by the Company in compliance with the Data Protection Act 2017 by electronically acknowledging my receipt on breatheHR by clicking on the blue tick button to mark the policy as read and accepted, hereby provide my consent.