As a Company Norman Lewis Business Equipment Ltd recognises that it has a legal duty of care towards protecting both employees and others who may be affected by the Company activities.

We reasonably believe we have undertaken all necessary action to ensure we are compliant with Data Protection guidelines as set out in legislation.
We have identified employees who potentially handle personal data including sensitive data and have ensured training has been provided to not only improve skills but mitigate risk associated.

The following sets out our Data Protection Policy.

Toni-Meri Coward

Toni-Meri Coward
Office Manager
On behalf of
Norman Lewis Business Equipment Ltd.

Data Protection Policy – GDPR

1. **Introduction**

1.1 This policy sets out how Norman Lewis Business Equipment Ltd ("we", "our", "us", "the Company") handles the personal data of our employees, workers and other third parties.

1.2 This policy 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, other individuals who work for us and those who apply to work for us (known technically as Data Subjects but for ease of reference we refer to them as "employees" in this policy).

1.3 Personal data means any information identifying a Data Subject (employee) or information relating to a Data Subject (employee) that we can identify (directly or indirectly) from that data. Examples are someone's salary details, working hours, work location, bank details, and emails about them or relating to them.

1.4 Processing means any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties

1.5 This policy applies to all Company staff including its employees, workers, contractors, agency workers, consultants, directors, and others.

1.6 You must read, understand and comply with this policy and attend training on its requirements. Any breach of this policy may result in disciplinary action.

2. **Scope**

2.1 The Company is committed to complying with data protection law including the principles set out in the General Data Protection Regulation (GDPR). We are exposed to large fines, and other legal liabilities if we breach of these principles.

2.2 All directors, managers, and supervisors are responsible for ensuring all staff comply with this policy.

2.3 The directors of the Company are responsible for developing this policy and for general compliance with data protection principles. See further section 10 of this policy.

2.4 We have appointed a Data Protection Officer (DPO) who is responsible for overseeing this policy. That post is held by **Toni-Meri Coward, our Office Manager.** She can be contacted on **toni.coward@normanlewis.com**

2.5 Please contact the DPO using the email address above if you have any questions about the operation of this policy or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

2.5.1 If you believe we may not have (or no longer have) a legal basis on which to process the personal data of an employee;

2.5.2 if you are unsure about the retention period for the personal data being processed (see section 6 below);

2.5.3 if you are unsure about what security or other measures you need to implement to protect personal data (see section 8 below);

2.5.4 if there has been a personal data breach (section 8 below);

2.5.5 if there are any queries or issues raised about someone's personal data.

2.5.6 If you receive a request for copies of personal data (see section 9 dealing with Subject Access Requests).

3. Personal Data Protection Principles

3.1 We adhere to the principles relating to processing of personal data set out in the GDPR, which require personal date to be:

3.1.1 Processed lawfully, fairly and in a transparent manner (see section 4 below).

3.1.2 Collected only for specified, explicit and legitimate purposes (see section 5 below).

3.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (see section 6 below).

3.1.4 Accurate and where necessary kept up to date (see section 7 below).

3.1.5 Not kept in a form which permits identification of employees for longer than is necessary for the purposes for which the data is processed (see section 6 below).

3.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (see section 8 below).

3.1.7 Not transferred to another country without appropriate safeguards being in place.

3.1.8 Made available to employees and employees allowed to exercise certain rights in relation to their personal data (see section 9 below).

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (see section 10 below).

4. Lawfulness, Fairness, Transparency

4.1 Personal data must be processed lawfully, fairly and in a transparent manner and only for specified purposes. These include where processing is necessary for the performance of the employment contract or to meet our legal compliance obligations or where we have a legitimate interest. We have formulated areas where we consider that we are entitled to process personal data relating to our staff and this information is set out in our privacy notices.

4.2 All managers are responsible for satisfying themselves that there is a proper legal basis for us to process personal data and to ensure that an appropriate privacy notice has been provided to all the employees they are responsible for. Any queries in this regard must be raised with the DPO.

4.3 The GDPR requires the Company to provide detailed, specific information through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an employee can easily understand them. This includes the identity of the data controller (ie the Company) and DPO, how and why we will use, process, disclose, protect and retain that personal data. The privacy notice must be presented when the employee first provides the personal data. This will usually mean both at the job application stage (in relation to the data necessary for that process) and at the time an employment contract is entered into.

4.4 When personal data is collected indirectly (for example, from a third party or publically available source), we must provide the employee with all the information required by the GDPR as soon as possible after collecting/receiving the data. We must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

5. **Purpose Limitation**

5.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes for example bank details collected for the purposes of paying staff should not be passed to our pension provider without the consent of the employee.

5.2 You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the employee of the new purposes and they have consented where necessary.

6. **Data Retention**

6.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

6.2 You may only process personal data when performing your job duties actually requires it. You cannot process personal data for any reason unrelated to your job duties.

6.3 Do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes. If in doubt seek guidance from your manager or the DPO**.**

6.4 You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention policy.

6.5 The Company will maintain a data retention policy and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with this policy.

7. **Accuracy**

7.1 Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

7.2 You will ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. All managers are responsible for checking the accuracy of any personal data at the point of collection and at regular intervals afterwards.

8. **Security, Confidentiality and Data Breaches**

8.1 Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

8.2 The Company will develop and maintain appropriate safeguards and will regularly test the effectiveness of those safeguards to ensure security of our processing. However, all staff have their part to play in helping to ensure that personal data is kept secure and that there are no data breaches. For example:

8.2.1 Be careful when responding to any requests from outside of the Company for any information about staff – always think is there a legitimate basis to respond to the request and is it covered by our privacy notice?

8.2.2 Ensure that personal information is not left on desks or where it can be seen by others;

8.2.3 Always use screensavers and passwords on PCs so that information on your screen cannot be seen by others;

8.2.4 Staff information should always be kept on a personnel file – and when information is removed from the file it should be returned promptly. Copies of information removed should be deleted as soon as it is no longer needed;

8.2.5 Personnel files should be kept locked in a filing cabinet and only accessed by an appropriate manager;

8.2.6 Emails containing personal information about staff should be deleted once they have been actioned unless it is necessary to keep the information on the personnel file – seek guidance if you are unsure.

8.2.7 Always check carefully when staff information is to be passed to a third party for example an occupational health provider, insurer, doctor, benefits provider, pension provider, security company – is this activity covered by the privacy notice and would such passing of information be allowed? If in doubt discuss with your manager or our DPO.

8.2.8 Under no circumstances should any photograph be taken of employee's passports on any Disclosure and Barring Service (DBS) certificates on any personal or company mobile phones, nor should any images be sent via Whats App or text. Instead a secure App will be used where it is necessary to send such information. Such information should only be sent to HR.

8.3 You must comply at all times with the requirements of our IT and Information Policy.

8.4 You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

8.5 The GDPR requires the Company to notify any personal data breach to the applicable regulator and, in certain instances, to the employee concerned.

8.6 We have put in place procedures to deal with any suspected personal data breach and will notify employees or any applicable regulator where we are legally required to do so.

8.7 If you know or suspect that a personal data breach has occurred, contact the DPO immediately. If you are unsure, please seek guidance and do not ignore such a situation.

9. Employees Data Rights and Requests

9.1 Employees have rights when it comes to how we handle their personal data. These include rights to:

9.1.1 withdraw consent to processing at any time;

9.1.2 request access to their personal data that we hold by way of a Subject Access Request;

9.1.3 ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

9.1.4 object to decisions based solely on automated processing, including profiling, for example an entirely online job application process;

9.1.5 make a complaint to the supervisory authority;

9.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

9.3 You must immediately forward any Subject Access Request you receive to HR. If in doubt whether a request has been made please speak to HR.

10. Accountability

10.1 The Company must implement appropriate measures to ensure compliance with data protection principles. To do this it has appointed a DPO who together with our board of directors is responsible for compliance.

10.2 The GDPR requires us to keep full and accurate records of all our data processing activities and a suitable log will be maintained by our DPO.

10.3 The Company is committed to providing appropriate training to its manager and all its staff in relation to its data protection obligations including those under GDPR. All staff must undergo all mandatory data privacy related training and managers must ensure that their team undergoes similar mandatory training.

10.4 Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

10.5 You may only share the personal data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

10.6 You may only share the personal data we hold with third parties, such as our service providers if:

10.6.1 they have a need to know the information for the purposes of providing the contracted services;

10.6.2 sharing the personal data complies with the privacy notice provided to the employee and, if required, the employee's consent has been obtained;

10.6.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

Dated: 04.10.2022