BEE ACTIVE

BEE ACTIVE CHILDCARE

SHOW STOPPERS

hivelink

General Data Protection Regulation (GDPR) Policy

Purpose of this Policy
Our GDPR Policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.

At Learn and Move Group Ltd we are committed to ensuring that we comply with the data protection principles, as listed below:

- Meeting our legal obligations as laid down by the Data Protection Act 2018;
- Ensuring that data is collected and used fairly and lawfully;
- Processing personal data only in order to meet our operational needs or fulfil legal requirements;
- Taking steps to ensure that personal data is up to date and accurate;
- Establishing appropriate retention periods for personal data;
- Ensuring that data subjects' rights can be appropriately exercised;
- Providing adequate security measures to protect personal data;
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues;
- Ensuring that all staff are made aware of good practice in data protection;
- Providing adequate training for all staff responsible for personal data;
- Ensuring that everyone handling personal data knows where to find further guidance;

• Ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly;
• Regularly reviewing data protection procedures and guidelines within the organisation.

Scope of this Policy

This policy applies to all employees and members of staff of The Learn and Move Group. This policy is not a stand-alone document but is supported by operational policies, procedures and processes. This policy will remain in force until notification is issued of the policy being superseded by an appropriately approved new version.

The scope of the Policy extends to obligations imposed by:

- Statutory and regulatory requirements;
- Learn and Move Group policies, standards, procedures and compliance plans;
- Relevant industry codes of conduct and practice notes.

This policy applies to any information kept on staff, customers and account holders including;

- Parent information – Full name, home address and postcode, telephone number, email address
- Participant information – Full name, date of birth, home address and postcode, age, gender, ethnicity, school attended, medical, dietary and safeguarding information and media consent.
- Booking information – Historical, current and future orders
- Staff information – Full name, home address and postcode, telephone number, email address, next of kin details, employment history, employment terms and conditions (e.g. pay, hours of work, holidays, benefits, absence), education and qualifications, national insurance number, driving licence details, passport details, birth certificate, banking details, appraisals, health and medical conditions, disciplinary records.
- Applicants – Full name and CV information.

Policy Review Cycle

This Policy is to be reviewed on an annual basis or when there is a significant change to the business, which may impact this policy.

Key Personnel

Data Protection Officer	Bobby Mills	01782 205 915 ext. 101 / bobby@beeactive.co.uk
Compliance Manager	Tim Sanders	01782 205 915 ext. 133 / tim@beeactive.co.uk
Office Manager	Nikki Milford	01782 205 915 ext. 124/ nikki@beeactive.co.uk

Data Protection Principles

UK GDPR sets out seven key principles which lie at the heart of the general data protection regime which The Learn and Move Group endeavour to abide by.

- Lawfulness, fairness and transparency – *'Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject'*
- Purpose limitation – *'Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.*
- Data minimisation – *'Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'*
- Accuracy – *'Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'*
- Storage limitation – *'Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject'*
- Integrity and confidentiality (security) – *'Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'*
- Accountability – *'The Data Protection Officer shall be responsible for, and be able to demonstrate compliance relating to GDPR'*

We will only process personal data if one of the following is present, in accordance with Article 6 of the UK GDPR;

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone's life.

(e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Learn and Move Group GDPR Statement

You can access our Company statement on GDPR here: Learn and Move Group GDPR Statement. This aims to set out clear guidance on how we use personal data at The Learn and Move Group.

Staff, customers and account holder GDPR rights at The Learn and Move Group

1. The right to be informed – *individuals have the right to be informed about the collection and use of their personal data.*
2. The right of access – *individuals have the right to access and receive a copy of their personal data, and other supplementary information at all times.*
3. The right to rectification – *individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.*
4. The right to erasure – *individuals have a right to have personal data erased*
5. The right to restrict processing – *individuals have the right to request the restriction or suppression of their personal data*
6. The right to data portability – *individuals have the right to data portability, which allows them to obtain and reuse their personal data for their own purposes across different services*
7. The right to object – *individuals have the right to object the processing of their personal data in certain circumstances*
8. Rights in relation to automated decision making and profiling

Data breaches

All data breaches will be reported and documented by the Compliance Manager. However, not all data breaches are required to be reported to the ICO, only those that put individuals rights and freedoms at risk. Data breaches judged not to be high risk still need documenting as the Company will need to be able to justify not reporting it to the ICO.

For high risk data breaches the Data Protection Officer will inform the ICO as soon as possible, but no later than 72 hours after becoming aware of it.

Individuals concerned will be informed of the breach and the following information provided;

- The name and contact details of the data protection officer,
- A description of the likely consequence of the personal data breach; and
- A description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

The following advice will also be passed onto the individuals to protect them;

- Forcing a password reset
- Advising individuals to use strong, unique passwords; and
- To look out for phishing emails or fraudulent activity on their accounts.

Policy References and Supporting Material

Data Protection Act 2018

ICO – UK GDPR

Gov.uk – Regulation (E) 2016/679 of the European PArliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)