Data Protection Policy

This Policy describes how personal data must be collected, handled and stored to meet our data protection standards and to comply with the law.

Data Protection Law
The Data Protection Act 1998 (**DPA**) and General Data Protection Regulation (**GDPR**) (EU) 2016/679 describe how organisations, including ours, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. Under GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) 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 not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate (having regard to the purposes for which it is processed) is erased or rectified, without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary, for the purposes for which the personal data is 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, subject to implementation of the appropriate technical and organisational measures required by GDPR, in order to safeguard the rights and freedom of individuals; and

(f) 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.

Article 5(2) requires that "the controller (Emma Northmore and Roberta McClelland) shall be responsible for (and be able to demonstrate) compliance with the principles."

Policy Details
Staff and volunteers have a responsibility to respect the nature of any confidential information divulged to them, in the context of their work with us. Emma Northmore and Roberta McClelland have overall responsibility for ensuring compliance with this Policy and with the DPA/GDPR and for ensuring that staff and volunteers are trained in and follow the guidelines in this Policy.

Any personal or sensitive information held by us is held because consent has been given in the form of agreement via the enrolment and course sign up forms.

Responsibilities
Everyone who works for or with us has a responsibility for ensuring that data is collected, stored and handled appropriately. Each person who works for us and who handles personal data must ensure that it is handled and processed in line with this Policy and data protection principles. However, these people have key areas of responsibility:

Emma Northmore and Roberta McClelland are ultimately responsible for ensuring that we meet our legal obligations.

The **Data Protection Officer** is responsible for:

- reviewing all data protection procedures and related policies annually;
- handling data protection questions from staff and anyone else covered by this Policy;
- ensuring that all systems, services and equipment used for storing data meet acceptable security standards;
- performing regular checks to ensure security is functioning properly;
- ensuring any third-party services that we use to store/process data conforms to GDPR;
- dealing with requests from individuals to see the data held by us about them (also called "subject access requests"); and
- approving any data protection statements attached to communications, such as e-mails and letters.

Confidentiality and the protection of staff and volunteers
The DPA/GDPR applies to data relating to staff, job applicants and volunteers. It covers data held on computer and on paper.

Under the terms of the Act/GDPR data must be:

- held with express consent;
- needed for the performance of the undertaking or contract;
- necessary, in order to comply with a legal obligation;
- necessary to protect the member of staff or volunteer from some life-threatening matter;
- necessary for the purposes of the legitimate interests of the data controller.

In addition, personal data must be:

- adequate, relevant and not excessive in relation to the purposes for which it is processed (e.g. personnel files should not contain out of date or superfluous material) and should be regularly reviewed;
- accurate;
- not kept longer than necessary for the purposes for which it is processed; and
- kept securely to protect against unauthorised or unlawful processing or accidental loss or damage.

Records held relating to a member of staff/freelance worker may include:

- references and information obtained during recruitment;
- payroll, tax and national insurance information;
- job duties and responsibilities;
- health records;
- absence and holiday records;
- any disciplinary investigations and proceedings; and/or
- contact names and addresses.

We will store the following data in relation to students and/or parents/guardians:

- registration forms (including personal and contact details);
- photographs/videos (as per Photography/Filming Consent terms and conditions);
- observational notes on performance/progress of the students;
- safeguarding concerns.

To comply with GDPR guidelines, personal data will not be kept for longer than is necessary.

To comply with the DPA, we agree to:

- store personally Identifiable data, recorded on paper, securely in a locked drawer or filing cabinet, which is behind at least one locked door;
- store personally Identifiable data, recorded on a computer/device securely, ensuring at least two passwords and encryption, where possible;
- consider the purpose or purposes of why we hold the information and decide whether (and for how long) it needs to be retained;
- we will securely delete (or shred any hard copies of) information that is no longer required; and
- updating, archiving or securely deleting information every two years.

Sharing of Data
Information held will be used for our purposes only. However, from time to time, data may need to be disclosed to third parties to comply with legal obligations (e.g. for the Inland Revenue or local authority safeguarding team).

Please note that any data sent out by us remains our responsibility. We must, therefore, ensure that the information that we are sending is going to the correct recipient and we must also be mindful of what is being sent.

General Staff Guidelines

- The only people able to access data covered by this Policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, members of staff can request it from Emma Northmore or Roberta McClelland.
- Members of staff should keep all data secure by taking sensible precautions and following the guidelines.
- In particular, strong passwords must be used and they should never be shared. A strong password can contain a mixture of uppercase and lowercase letters, symbols and numbers (e.g. Pa55w0rd!).
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated as necessary.
- Staff should request help from the Data Protection Officer if they are unsure about any aspect of data protection.
- Staff's personal devices should not be used to hold/store data, **unless** the Data Protection Officer has checked that it has the right level of security and has agreed the use of the device.

Data Storage
These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Officer. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for whatever reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Staff members should make sure paper and printouts are not left where unauthorised people could see them (e.g. on a printer).
- Data printouts should be shredded and disposed of securely when no longer required.
- Personal/sensitive data which is stored on USB storage devices must be encrypted – the Data Protection Officer can provide an encrypted USB device, if required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should never be saved directly to laptops or other mobile devices (such as tablets or smart phones), unless said device is encrypted.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use
Personal data is of no value to us, unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, staff members should ensure that the screens of their computers are always locked when left unattended.
- If personal data needs to be transferred to a party outside of the EU, adequate protection needs to be enforced to safeguard the information. This is because the Data Protection Policy and the GPDR guidelines are only applicable to members of the EU (and the UK who agreed to the guidelines upon leaving the EU).

Data Accuracy
The law requires that we take reasonable steps to ensure that data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort we will put into ensuring its accuracy.

It is the responsibility of all staff who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets (copies).
- Staff should take every opportunity to ensure that data is updated. For instance, by confirming a customer's details when they call.
- We will make it easy for data subjects to update the information that we hold about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests
All individuals who are the subject of personal data held by us are entitled to:

- ask what information the company holds about them and why;
- ask how to gain access to it;

- be informed how to keep it up to date; and
- be informed how the company is meeting its data protection obligations.

If we are contacted by an individual requesting the information held by us, this is called a "subject access request".

Subject access requests from individuals should be made by e-mail and addressed to the data controller at
admin@balletboost.com

The data controller can supply a standard request form, although individuals do not have to use this. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Rights of Staff and Volunteers
A staff member or volunteer has the right to know what data is held about them and they are able to request an explanation as to the purposes for which information is held. They are also able to know the persons to whom it is disclosed and other details relating to processing. The staff member or volunteer must put any request in writing and have the right to have any inaccurate data corrected.

If any data is unlawfully used, the member of staff or volunteer can be compensated for damage caused by contravention of the DPA.

Emma Northmore and Roberta McClelland are ultimately responsible for ensuring that we meet our legal obligations and we agree to ensure all requirements are met and any necessary amendments that are needed due to GDPR are adhered to.

Please note that the policy and procedures set out above do not form part of staff members' contracts of employment or volunteers' terms of engagement and may be changed by us in our absolute discretion at any time.

Version number	1	**Date**	May 2018
Adopted on	1st May 2018	**By (full name)**	Emma Northmore
By (signature)	E.Northmore	**Next review date**	May 2019