MINDFUL
PEAK PERFORMANCE

Mindful Peak Performance CIC
Data Protection Policy

Definitions

Organisation	means Mindful Peak Performance CIC, a registered social enterprise.
GDPR	means the General Data Protection Regulation.
Responsible Person	Means Luke Doherty, Managing Director of Mindful Peak Performance CIC.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Charity.

1. Introduction

This policy is to satisfy the legal obligation of the Organisation to notify staff about the use of their personal data as well as their use of client's personal data. Proper data security rules instil confidence in clients and employees and help protect them and the organisation from any mishandling of personal data. This data protection policy outlines the responsible parties, the sorts of data covered, and the essential protection measures for the security of personal data.

2. How the Organisation will use this data protection and data security policy

- to inform staff/clients about the use of their personal data, as required by law.
- to educate staff/clients about the principles they must adhere to in handling personal data to help comply with the organisation's duty to protect the security of personal data, by informing staff/clients of necessary measures

Staff will be briefed as part of induction and given the policy. This policy is available upon request to clients and other interested parties, and is available via our website. Clients and other parties can opt out of receiving communications from the Organisation, and their data will be securely removed as soon as is reasonably possible.

3. Why data is collected by the Organisation

The Organisation collects and processes information in order to:

- Deliver services in line with social enterprise objectives
- Meet its obligations as an employer, and to its Board and volunteers and organisations and individuals from whom it obtains goods and services
- Satisfy the needs of funders/prospective funders and other partners
- Market services to people ie. send information about existing and new services
- Monitor and evaluate services
- Satisfy equal opportunities and diversity policies
- Take payments for services

4. Types of data collected by the organisation

The Organisation collects and processes the following types of data:

- **Staff:** the Organisation collects details including name, address, telephone number, email address, details of training and qualifications, DBS record, professional references and payment details.
- **Clients - companies:** the Organisation collects details including company name, address, staff contact details, payment information.
- **Clients - individuals:** the Organisation collects details including name, address, telephone number, email address, age, diversity and equality information (anonymised).
- **Partner organisations:** the Organisation collects details including partner name, address, telephone number, email address, individual contact names, details of relevant training and qualifications, DBS records, professional references.

5. The uses the Organisation makes of data concerning

The Organisation uses data in the following ways:

- **Staff:** data is used for employment, payment and safeguarding purposes.
- **Clients - companies:** the data is used to deliver the Organisation's social enterprise activities, receive payments and inform them of services.
- **Clients - individuals:** the data is used to deliver the Organisation's social enterprise

activities, inform them of services, provide information for funders or potential funders, and for safeguarding purposes.
- **Partner organisations:** data is used to work with partners to deliver the Organisation's social enterprise activities and for safeguarding purposes.

All this data is covered by the policy. Subject access requests can be made, and will be responded to by the Responsible Person as soon as is reasonably possible.

6. Data protection principles

The Organisation is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the 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 they are processed;
d. 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;
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 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms 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."

7. General provisions

a. This policy applies to all personal data processed by the Organisation.
b. The Responsible Person shall take responsibility for the Organisation's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Organisation is registered with the Information Commissioner's Office as an

organisation that processes personal data.

8. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Organisation shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the Organisation shall be dealt with in a timely manner.

9. Lawful purposes

a. All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Organisation shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems.

10. Data minimisation

a. The Organisation shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

11. Accuracy

a. The Organisation shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

12. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

13. Security

a. The Organisation shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. The Organisation shall ensure that hard copy personal data is stored securely under lock

and key until it can be transferred to digital copy (at the earliest reasonable time) and then is shredded.

c. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
d. When personal data is deleted this should be done safely such that the data is irrecoverable.
e. Appropriate back-up and disaster recovery solutions shall be in place.

14. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

We believe our privacy policy is fully compliant with GDPR.

Last updated	08 May 2021