Data Privacy and Protection Policy

Purpose

The objective of this policy is to ensure that:

- Personal Data is processed by Mye-coach in compliance with the requirements of GDPR 2018 and other relevant information governance legislation and
- Personnel are aware of their obligations when Processing Personal Data on behalf of Mye-coach

Definitions

1. Data Controller: the organisation (alone, jointly or in common with other organisations) which determines the manner and purposes for which Personal Data is to be processed.
2. Data Processor: processes data on behalf of the Data Controller (other than an employee).
3. GDPR 2018, together with all secondary legislation made under it. The mutually agreed General Data Protection Regulation (GDPR) came into force on May 25th 2018 and is designed to modernise laws that protect the personal information of individuals. It gives individuals certain rights regarding the information that is held about them and obliges Mye-coach to respond to any requests from an individual to access their own Personal Data.
4. Data Protection Principles: a set of statutory requirements, which all Data Controllers are obliged to adhere to. The Principles balance the legitimate need for organisations such as Mye-coach to process Personal Data against the need to protect the privacy rights of the Data Subject.
5. Data Subject: an individual who is the subject of Personal Data.
6. Human Rights Act (HRA): the Human Rights Act 1998.
7. Information Commissioner: the regulator appointed by the Crown to promote public access to official information and protect personal information. Compliance with the DPA is enforced by the Information Commissioner.
8. Information Governance: a business unit within Mye-coach.
9. Information Management (IM): a unit within Mye-coach.
10. Information Owners: senior managers, who are responsible for the acquisition, creation, maintenance and disposal of Mye-coach's information and Information Systems within their assigned area of control.
11. Internal Audit: a business unit within Mye-coach.
12. Personal Data: information which relates to a living individual who can be directly identified from either the information itself, or by combining the information with

other data available to Mye-coach. Personal Data includes expressions of opinion and indications of intention, as well as factual information.

13. Privacy Risk: that part of Mye-coach's overall risk portfolio which relates to the, integrity, availability and confidentiality of Personal Data within Mye-coach.
14. Processing/Processed: includes collecting, recording, storing, retrieving, transmitting, amending or altering, disclosing, deleting, archiving and destroying Personal Data.
15. Subject Access Request: a request from an individual for access to their Personal Data.
16. Mye-coach Personnel: includes all Mye-coach employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as Data Processor, confidentiality or non-disclosure agreements) have been made.

Organisational scope

This policy applies to all Mye-coach Personnel and to all Data Processed by Mye-coach at any time, by any means and in any format.

Policy statement

1. Mye-coach will comply with GDPR and adhere to the core Principles, as described here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

2. A number of criminal offences are defined in GDPR:

    - Knowingly or recklessly obtaining or disclosing Personal Data without the consent of the Data Controller
    - Procuring the disclosure to another person of Personal Data without the consent of the Data Controller
    - Repeatedly and negligently allowing Personal Data to be disclosed
    - Intentionally or recklessly failing to comply with the Data Protection Principles and
    - Altering, defacing, destroying or concealing data in order to prevent disclosure. The discovery or suspicion that one of these offences may have been committed must be reported to the Privacy and Data Protection Team within Information Governance, so that they can determine whether or not the matter should be referred to the police and/or the Information Commissioner

3. Mye-coach will comply with the statutory requirement to maintain an accurate entry on the Information Commissioner's public register of Data Controllers which describes the purposes for which Personal Data is processed.

4. Mye-coach will comply with other relevant legal requirements where they apply to its processing of Personal Data, including:

    - The Human Rights Act and the requirement to act in a way which is compatible with the right to respect for private and family life in the European Convention of Human Rights and Fundamental Freedoms
    - The Privacy and Electronic Communications (EC Directive) Regulations 2003
    - The common law duty of confidence

5. Mye-coach will adhere to the requirements set out in the following standards, policies and guidance in order to support its compliance with GDPR:

    - The Information Commissioner's suite of guidance documents and Codes of Practice
    - The Payment Card Industry Data Security Standard (PCI DSS)
    - Mye-coach's Policy on the Disclosure of Personal Data to the Police and other Statutory Law Enforcement Agencies
    - Mye-coach's Information and Records Management Policy
    - Mye-coach's Information Security Policy

Policy content

1. Mye-coach's policy is to ensure that:

    - It has in place structures, systems and processes to manage all Personal Data fairly and lawfully and in a way that ensures its integrity, accuracy, relevance and security

    - In response to a valid Subject Access Request, Mye-coach will tell a Data Subject whether it, or someone else on its behalf, is processing that individual's Personal Data, and if so, provide a description of: the Personal Data; the purposes for which they are being processed; and those to whom they have been, or may be, disclosed. Mye-coach will also communicate in an intelligible form, the information which forms any such Personal Data

    - Mye-coach will respond to all Subject Access Requests within 15 calendar days of receipt of a valid request

- In response to a Subject Access Request, Mye-coach will only refuse to provide a copy of the Personal Data which it is Processing (and any associated information concerning its processing) if a statutory exemption applies. Any such refusal must be approved by Information Governance;

- Personal Data used for communicating with Mye-coach's customers will be treated in accordance with the preferences they have expressed

- Any activity intended to monitor an employee's activities in the workplace which may involve the disclosure of Personal Data or interference with the right to a private life, must be carried out in accordance with GDPR, the HRA, other relevant legislation and any duty of confidence which is owed

- Personal Data will not be disclosed to third parties except where disclosures are permitted by, or required by, law

- Personal Data will be labelled in accordance with Mye-coach's Information Security Classification Standard for protectively marking Information

- Procurement processes and contractual arrangements with external service providers must include adequate measures to ensure compliance with the Data Protection Principles and associated requirements outlined in this policy

- Privacy Risk will be considered and afforded a priority in decisions within Mye-coach in the same way as financial and operational risk. Privacy Risk will be managed by a process of identifying, controlling, minimising and/or eliminating risks that may affect Mye-coach's Processing of Personal Data

- Any complaint about Mye-coach's non-compliance with the standards set out in this Privacy and Data Protection Policy must be promptly directed to the Management Team. The complaint will be dealt with in accordance with Mye-coach's Privacy and Data Protection Complaints Handling Procedure, however Mye-coach recognises that individuals will also have the right to take their complaint directly to the Information Commissioner or, in certain circumstances (as defined in the DPA), the courts

Responsibility for compliance

1. All Mye-coach Personnel are responsible for actively supporting compliance with this policy.

2. Mye-coach employees involved in the Processing of Personal Data must familiarise themselves with the supporting guidance available on the Mye-coach Management System and Intranet.

3. Information Owners are responsible for:

    - Ensuring that Mye-coach Personnel within their area of control are aware of this policy and are adequately trained in the handling of Personal Data
    - The assessment and reporting of Privacy Risk linked to the Processing of Personal Data within their area of control
    - Implementing appropriate procedures to ensure compliance with restrictions on the Processing of Personal Data within their area of control

4. Management Team is responsible for:

    - Providing advice and guidance on the implementation and interpretation of this policy
    - Promoting and enforcing compliance with this policy
    - Investigating and resolving complaints about Mye-coach's non-compliance with GDPR and/or this Policy
    - Liaising with the Information Commissioner's Office on any matter relating to Mye-coach's compliance with GDPR and/or this policy
    - Maintaining Mye-coach's entries on the Information Commissioner's public register of Data Controllers

5. Information Governance, Internal Audit and IM are responsible for managing and investigating any actual or suspected unauthorised disclosures of Personal Data and recommending measures to prevent the reoccurrence of such incidents and breaches;

6. IM is responsible for advising the business on the technical measures and controls required to protect the security of Personal Data Processed by Mye-coach using electronic information and communications systems;

7. Internal Audit is responsible for auditing the business processes, operating procedures and working practices of Mye-coach and its service providers which affect the Processing of Personal Data, to monitor compliance with this policy.