Data Breach Policy for M40 Offices

Purpose: This policy outlines the procedures and responsibilities of M40 Offices ("Controller") in the event of a personal data breach in accordance with the General Data Protection Regulation (GDPR).

Definitions

- "Personal data" refers to any information relating to an identified or identifiable natural person as defined in the GDPR.
- "Data breach" refers to the unauthorised or unlawful processing of personal data, including accidental or intentional loss, destruction, alteration, unauthorised disclosure, or access.
- "Data Protection Officer" refers to the individual appointed by the Controller to oversee data protection and data breach management.

Responsibilities

1. **Data Protection Officer**: The Data Protection Officer shall be responsible for ensuring that the Controller has in place appropriate technical and organisational measures to prevent personal data breaches, as well as for managing personal data breaches and ensuring compliance with the GDPR.
2. **Employees**: All employees shall be responsible for ensuring the confidentiality, integrity, and availability of personal data and reporting any suspected data breaches to the Data Protection Officer.
3. **Third-party processors**: The Controller shall ensure that third-party processors engaged for the processing of personal data on behalf of the Controller have in place appropriate technical and organisational measures to prevent personal data breaches, and that they are obligated to inform the Controller in the event of a personal data breach.

Procedure

1. **Notification**: The Controller shall notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. The Controller shall provide the ICO with the following information:

    - Description of the nature of the personal data breach, including categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected.
    - Contact details of the Data Protection Officer.
    - Description of the likely consequences of the personal data breach.
    - Description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.

2. **Investigation**: The Data Protection Officer shall conduct an investigation into the personal data breach and determine its cause and potential consequences.
3. **Notification to Data Subjects**: The Controller shall inform the data subjects without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms. The notification shall include the following information:

    - Description of the nature of the personal data breach.
    - Contact details of the Data Protection Officer.
    - Description of the likely consequences of the personal data breach.

- Description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.
- Advice on appropriate steps the data subjects can take to protect themselves from potential adverse effects of the personal data breach.

4. **Mitigation**: The Controller shall take appropriate measures to address the personal data breach and minimise its potential adverse effects.
5. **Documentation**: The Controller shall document any personal data breaches, including the facts relating to the personal data breach, its effects, and the remedial action taken.

Training and Awareness

The Controller shall provide training and raise awareness among employees and third-party processors on data protection and data breach management, including the procedures outlined in this policy.

Review

This policy shall be reviewed annually and updated as necessary to ensure that it remains compliant with the GDPR and reflects the evolving needs of the Controller.

Review Date	Reviewed By	Comments
08/03/2023	Jake	Creation of document