QMB Group LTD Data Protection Policy

1. Data protection principles

The QMB Group LTD 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 tonsure 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."

2. General provisions

a. This policy applies to all personal data processed by the QMB Group LTD.

b. The Responsible Person shall take responsibility for the QMB Group LTD ongoing compliance with this policy.

c. This policy shall be reviewed at least annually.

d. The QMB Group LTD shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the QMB Group LTD 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 QMB Group LTD shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the QMB Group LTD must be done on one of the following lawful basis: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

b. The QMB Group LTD 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 QMB Group LTD's systems.

5. Data minimisation

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

6. Accuracy

a. The QMB Group LTD 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.

7. Communication and CPD

Communication:

a. **Confidentiality**: This section emphasizes the importance of maintaining the confidentiality of personal data during communication. It states that all staff members should keep personal data confidential and should only disclose it to authorized individuals who have a legitimate need to know. This means that personal data should not be shared with anyone who does not require access to that information for their job responsibilities.

b. **Secure Communication Channels:** To protect personal data from unauthorized access or interception, staff members are required to use secure and encrypted methods when transmitting data through communication channels. Encryption ensures that the information being transmitted is encoded and can only be deciphered by authorized recipients who possess the decryption key.

c. **Email Usage**: This section specifically addresses the use of email for communication. Staff members are advised to exercise caution to avoid unintentionally disclosing personal data. They should not include personal data in the subject line of an email, as this can be easily visible to unauthorized recipients. Furthermore, personal data should only be shared with individuals who are authorized to receive it.

Training and CPD

a. **Data Protection Awareness:** This section focuses on training and continuous professional development (CPD). It states that all staff members should receive appropriate training and awareness programs regarding data protection and privacy best practices. The purpose of this training is to ensure that employees understand their responsibilities under the data protection policy and are aware of any changes in data protection laws or internal policies.

b**. Use of Personal Data:** During training or CPD activities, staff members may come into contact with personal data for instructional purposes. This section emphasizes that personal data should only be used to the extent necessary to achieve the training objectives. Staff

members should not store, share, or use the personal data for any other purpose without proper authorization.

c**. Security of Training Materials:** Training materials and resources that contain personal data should be stored securely, both in physical and digital formats. Access to these materials should be restricted to authorized personnel only. This helps prevent unauthorized individuals from accessing or misusing personal data included in the training materials.

d**. Consent and Privacy:** Staff members are required to obtain appropriate consent from individuals whose personal data may be used during training or CPD activities. Participants should be informed about the purpose of data collection, how their data will be used, and their rights regarding the processing of their personal information. This ensures transparency and respects individuals' privacy rights.

8. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the QMB Group LTD 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.

9. Records

This policy outlines the arrangements for retaining accurate records of internal assessments for a period of 12 months from the certification date.

Purpose of Retaining Records: The retention of accurate records of internal assessments is essential to demonstrate our commitment to data protection and compliance. These records serve as evidence of our continuous improvement efforts, ensuring that we maintain robust data protection practices and fulfill our obligations under relevant data protection laws.

Records Retention Period: All records of internal assessments, including assessment reports, findings, action plans, and related documentation, will be retained for a minimum period of 12 months from the date of certification. This period allows for effective monitoring, auditing, and review of our data protection practices.

Storage and Access: The records of internal assessments will be securely stored in a designated repository or document management system, accessible only to authorized

personnel who have a legitimate need to access such information. Measures will be implemented to protect these records from unauthorized access, loss, alteration, or destruction.

Accuracy and Integrity: We will ensure that the retained records of internal assessments are accurate, complete, and up to date. Any modifications or updates made to these records during the retention period will be clearly documented, including the reasons for the changes and the individuals responsible for the modifications.

Disposal of Records: After the 12-month retention period, records of internal assessments will be disposed of securely and in accordance with our data retention and disposal policies. Any personal data contained within these records will be anonymized or pseudonymized, where possible, to protect individuals' privacy.

Review and Audit: Regular reviews and audits will be conducted to verify the accuracy and completeness of the retained records of internal assessments. These reviews may be performed by our internal data protection team, external auditors, or regulatory authorities to assess our compliance with data protection regulations.

Legal and Regulatory Requirements: Our retention of accurate records of internal assessments is in accordance with applicable legal and regulatory requirements, including but not limited to the General Data Protection Regulation (GDPR) and other relevant data protection laws in our jurisdiction.

Training and Awareness: All employees and relevant stakeholders will receive appropriate training and awareness programs to understand the importance of retaining accurate records of internal assessments. They will be educated on their roles and responsibilities regarding the documentation and storage of these records.

Continuous Improvement: We are committed to continuous improvement in our data protection practices. The records of internal assessments will be used to identify areas for improvement, implement corrective actions, and monitor the effectiveness of our data protection measures.

10. Security

a. The QMB Group LTD shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

b. 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.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

11. 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 QMB Group LTD shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO

12. Information to Awarding Bodies

It is the responsibility of the Centre Coordinator to ensure all information provided to the Awarding Body is accurate and complies with the General Data Protection Regulations. The student Application form will be submitted to the Awarding Body which will have the candidate's data. This will include;

- full name
- date of birth
- gender
- home address