

# Data Protection Policy

## Methody Collegians

|              |         |
|--------------|---------|
| Last updated | 19SEP24 |
|--------------|---------|

### Definitions

|                            |  |
|----------------------------|--|
| <b>Organisation</b>        | means Methody Collegians   |
| <b>DPA</b>                 | means the Data Protection Act 2018 which implements the EU's General Data Protection Regulation.     |
| <b>Responsible Person</b>  | Means Joanne Mehaffy (Membership Secretary)  |
| <b>Register of Systems</b> | means a register of all systems or contexts in which personal data is processed by the Organisation. |

### 1. Data protection principles

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

DPA 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 DPA 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 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 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 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.

## **4. 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.

## **5. 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.

## 6. 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.

## 7. 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.

## 8. Security

- a. The Organisation 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.

## 9. 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 ([more information on the ICO website](#)).



## **Appendix 1**

### **Register of Systems**

All data is stored on the Whitefuse platform in accordance with the Data Processing Terms.

Data is held on this platform following affirmative consent.

Users are responsible for keeping their own data up to date via the secure membership portal.

### **Archiving Policy**

- Active Members – data will be retained for the life of the membership.
- Lapsed Members – data will be retained for a period of 1 year to allow for renewal and then will be deleted.
- Friends of MCB – data will be retained for the life of the membership, with additional communications regarding removal requests sent annually.
- Event Attendees – name, email address and event history will be retained for a maximum period of 3 years to allow for notification of similar rolling events
- Donors – name, email address and donation details held for 6 years for financial reporting and then will be deleted.

### **Security Policy**

All data is stored on the Whitefuse platform. To ensure that the data is safe and secure it is hosted within the EU on a highly scalable hosting infrastructure. A range of automated tests, checks and backups ensure reliability and the cloud-based nature of the product ensures that Methody Collegians always using the very latest version of the software.

Access to the full database is limited to those with approved Administrator Access which includes Members of the Methody Collegians Council and Staff within the Methodist College Belfast Alumni Relations Office.

Exports of data are controlled via password protection, only shared within the Methodist College Belfast staff network or the Methody Collegians Council, and deleted after use.

Access to Member Directories is available to those with a valid membership subscription who have declared that they will comply with the Terms of Membership

Data held in the Member Directories is done so by affirmative consent.

