

## OMC Data Protection Policy

### Principles:

1. The OMC's data protection policy draws on the best practice guidance from the University of Oxford.
2. The policy covers the handling and usage of all customer data, including email addresses and personal information.
3. The intention of the policy is to outline that the OMC holds the protection of customer data very seriously.
4. We will publicly state our principles on our website terms and conditions.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal information provided to the OMC will only be used for the purposes stated when the information is requested. Personal information will not be given to third parties without consent of the individual concerned. Personal information collected and/or processed by the OMC is held in accordance with the provisions of the General Data Protection Regulation.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. The GDPR provides individuals with rights in connection with personal data held about them. It provides individuals with the right to access data concerning themselves. The OMC will provide individuals with this information if requested.
9. The OMC will ensure that data held is kept with appropriate levels of security, for example electronic data may be either encrypted or password protected as appropriate. Access to personal data will be kept to the minimum number of users. Users will follow the guidance in usage of data and be made aware of this through the training process or through work contracts.
10. All staff or other individuals who have access to, or who use, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised person.
11. Staff and other individuals should be aware that guidelines and regulations relating to the security of manual filing systems and the preservation of secure passwords for access to relevant data held on computer should be strictly observed.
12. Staff will be trained on the data protection policy and the OMC will ensure updated training is in place as required.

13. Disposal of files and other similar material - manual records and other materials which are of a confidential nature should not be allowed to pass into the public domain either deliberately or accidentally. Special care needs to be taken in disposing of all waste material, by arranging for the material to be shredded through the appropriate channels as advised by the OMC.
14. When a customer visits the OMC website, their computer may be issued with a small file (a cookie) for the purposes of managing and improving the services on the website. Cookies do not contain any personally identifying information, but is used to assist with monitoring traffic on the website through Google Analytics. Demographical and statistical information about user behaviour may be collected and used to analyse the popularity and effectiveness of the OMC's website. Any disclosure of this information will be in aggregate form and will not identify individual users.
15. A failure to comply with the provisions of the GDPR may render the OMC, or in certain circumstances the individuals involved, liable to prosecution as well as giving rise to civil liabilities.
16. Further Information from OMC  
Questions about this policy should be directed to [admin@oxfordmindfulness.org](mailto:admin@oxfordmindfulness.org)

## **1. Purpose and scope**

This policy provides a framework for ensuring that the OMC meets its obligations under the General Data Protection Regulation (GDPR) and associated legislation ('data privacy legislation'). It applies to all processing of personal data carried out for an OMC purpose, irrespective of whether the data is processed on OMC equipment or by third parties.

'Personal data' means any information relating to an identifiable living individual who can be identified from that data or from that data and other data. 'Processing' means anything that is done with personal data, including collection, storage, use, disclosure and deletion.

More stringent conditions apply to the processing of special category personal data. 'Special category' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

## **2. Principles**

The processing of personal data must comply with data privacy legislation and, in particular, the six

data privacy principles. In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner;
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, up-to-date;
- not kept for longer than necessary; and
- kept safe and secure.

In addition, a new accountability principle requires us to be able to evidence compliance with these principles.

### **3. Aims and commitments**

The OMC handles a large amount of personal data and takes seriously its responsibilities under data privacy legislation. It recognises that the mishandling of an individual's personal data may cause them distress or put them at risk of identity fraud. As a result, it is committed to:

- complying fully with data privacy legislation;
- where practicable, adhering to good practice, as issued by the ICO or other appropriate bodies; and
- handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.

The OMC seeks to achieve these aims by:

- ensuring that staff, students and other individuals who process data for OMC purposes are made aware of their individual responsibilities under data privacy legislation and how these apply to their areas of work. For example, employment contracts include a clause drawing the attention of the employee to data privacy legislation and the OMC's data protection policy;
- providing suitable training, guidance and advice.

### **4. Breaches of data privacy legislation**

The OMC will investigate incidents involving a possible breach of data privacy legislation in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future. Depending on the nature and severity of the incident, it may also be necessary to notify the individuals affected and/or the ICO. A breach will occur where, for example, personal data is disclosed or made available to unauthorised persons or personal

data is used in a way that the individual does not expect. Incidents involving failures of IT systems or processes must be reported to OMC CEO immediately of discovery. OMC will liaise, as appropriate, with the Information Compliance Regulator.

## **5. Compliance**

The OMC regards any breach of data privacy legislation, this policy or any other policy and/or training as a serious matter, which may result in disciplinary action or (in the case of self-employed contractor) termination of engagement. Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of the OMC to disclose personal information unlawfully).

END