THE MAALOS KEDOSHIM UOHC MIKVAH PRIVACY POLICY

Introduction

The Woodstock Mikvah Limited otherwise known as The Maalos Kedoshim UOHC Mikvah (we", "us" or "TWML") takes the security of data held by us in relation to customers, staff and other individuals, very seriously. TWML staff and volunteers have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures set out in this policy.

TWML gather and use information about individuals including volunteers and those using its services when required. This data contains "personal data" and "sensitive personal data" (known as "special categories of personal data" under the GDPR).

This policy sets out our duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

Legislation

It is a legal requirement that we process data correctly; we must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

The Data Protection Act 1998

The General Data Protection Regulation (EU) 2016/679 (the GDPR)

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications)

Any other legislation that, in respect of the United Kingdom (UK), replaces, or enacts into UK domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the UK leaving the European Union.

Data

We hold a variety of data relating to individuals, including staff, volunteers and service users (also referred to as "data subjects") which is known as personal data.

Personal data is information by which a living individual can be identified either by that data alone, or in conjunction with other data held by us.

Processing of personal data

We are permitted to process personal data on behalf of data subjects provided it is doing so on one of the following grounds:

- processing with the consent of the data subject
- processing is necessary for the performance of a contract between us and the data subject or for entering into a contract with the data subject;
- processing is necessary for our compliance with a legal obligation;
- processing is necessary to protect the vital interests of the data subject or another person; or

- processing is necessary for the purposes of legitimate interests.

1. Employees and volunteers

Employee personal data and, where applicable, special category personal data or sensitive personal data, is held and processed by us. A copy of any employee's personal data held by us is available upon written request by that employee from the Directors.

2. Consent

We may use consent as a ground of processing but usually where no other alternative ground for processing is available. Consent shall always be obtained in writing and freely given by the data subject.

3. Processing of special category personal data or sensitive personal data

If we process special category personal data or sensitive personal data, this must be done on with one of the following grounds of processing:

- the data subject has given explicit consent to the processing of this data for a specified purpose
- processing is necessary for carrying out obligations or exercising rights related to employment or social security
- processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person
- processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity
- processing is necessary for reasons of substantial public interest.

4. Data Sharing

We share our data with various third-parties. To enable us to ensure compliance by these third-parties with data protection laws, we will require the third-party organisations to enter in to an agreement with us to govern the processing of data, security measures to be implemented and responsibility for breaches.

If personal data is shared between us and third-parties who require to process personal data that we process as well, then both us and the third-party will be processing that data in their individual capacities as data controllers.

Where we share in the processing of personal data with a third-party organisation (e.g. for processing of the employees' pension), we shall require the third-party organisation to enter in to a data sharing agreement with us.

5. Data processors

A data processor is a third-party that processes personal data on behalf of us or if parts of our work is outsourced (e.g. payroll, maintenance and repair works).

A data processor must comply with data protection laws and ensure they have appropriate technical security measures in place, maintain records of processing activities and notify us if a data breach is suffered.

If a data processor wishes to sub-contact their processing, they will require our prior written consent. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

Data storage and security

All personal data whether held electronically or in paper format, must be stored securely.

1. Paper storage

Personal data stored on paper must be kept in a secure place and only accessed by authorised persons. No personal data must be left around where it could be seen by unauthorised persons. All personal data which is no longer required, must be disposed of and destroyed. Any paper files which need to kept in that format and cannot be scanned, should be stored in accordance with our Data Security Policy.

2. Electronic storage

Personal data stored electronically must also be protected from unauthorised use or access. Personal data must be password protected when being sent internally or externally to our data processors or those with whom we have entered in to a data sharing agreement. If personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

Breaches

We take the security of personal data seriously and if a data breach should occur, then we have to follow reporting duties.

In the event that a breach or potential breach has occurred, and no later than six (6) working hours after it has occurred, the data protection officer (DPO) must be notified in writing (or by email) of the breach, how it occurred, the likely impact of that breach is on any data subject(s).

It is vital to seek to contain the breach by whatever means available.

The DPO must consider whether the breach is one which requires to be reported to the Information Commissioner's Office (ICO) and to the data subjects affected.

The DPO should notify third parties in accordance with the terms of any applicable data sharing agreements.

The DPO is required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of the breach to the ICO within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

Data protection officer

A DPO is an individual who has an over-arching responsibility and oversight over compliance by us with data protection laws.

The DPO will be responsible for:

Monitoring our compliance with data protection laws and this policy and co-operating with and serving as our contact for discussions with the ICO, and for reporting breaches or suspected breaches to the ICO and data subjects.

Data subject rights

Data subjects are entitled under the GDPR to view the personal data held about them by us, whether in written or electronic form.

Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to our processing of their data.

1. Subject access requests

Data subjects are permitted to view their data held by us upon making a request to do so (a subject access request). Upon receipt of a request by a data subject, we must respond to the subject access request within one month of the date of receipt of the request.

We must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.

Where the personal data comprises data relating to other Data subjects, we must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the subject access request.

Where we do not hold the personal data sought by the data subject, must confirm that we do not hold any personal data sought by the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

2. The right to be forgotten

A data subject can exercise their right to be forgotten by submitting a request in writing to us seeking that we erase the data subject's personal data in its entirety.

Each request received by us will require to be considered on its own merits and legal advice may be required in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with this clause and will respond in writing to the request.

3.The right to restrict or object to processing

A data subject may request that we restrict our processing of the data subject's personal data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time to time by us, a data subject has an absolute right to object to processing of this nature by us, and if we receive a written request to stop processing for this purpose, then we must do so immediately.

Each request received by us will require to be considered on its own merits and legal advice may be required in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request and will respond in writing to the request.