DATA PROTECTION POLICY

1. Purpose

MOHS Workplace Health (MOHS) takes the security and privacy of your data extremely seriously, but we need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We are committed to complying with all the data protection legal obligations.

This policy sets out our obligations regarding data protection and the rights of suppliers, contractors, consultants, customers and business contacts ('data subjects') in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ('GDPR'). If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside any contract for services and/or any other notice we issue to you from time to time in relation to your data.

MOHS has taken steps to protect the security of your data and trains our employees about their data protection responsibilities as part of the induction process. We will only hold data for as long as necessary for the purposes for which we collected it.

The parties acknowledge that for the purposes of the data protection legislation, the 'customer' is the data controller and MOHS is the 'data processor' (where data controller and data processor have the meanings as defined in the data protection legislation).

This policy explains how MOHS will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working with MOHS.

The customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the personal data to MOHS which, for the avoidance of doubt, includes but is not limited to all necessary consents from its employees and workers, for the duration and purposes of this agreement.

2. Data protection principles

Personal data must be processed in accordance with six 'General Data Protection Principles'.

It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3. How we define personal data

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as your employer) or it could be created by us. It could also be provided or created during the course of the contract of services or after its termination.

The types of personal data we collect and use about you is included in the Privacy policy that is available on request from our data protection officer (DPO) Helen Hooper.

4. How we define special categories of personal data

'Special categories of personal data' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data, as detailed in the privacy policy, in accordance with the law.

5. How we define processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6. How will we process your personal data

MOHS shall, in relation to any personal data processed in connection with its performance of its obligations under this agreement:

- process personal data only on the written instructions of the customer unless MOHS is required by the laws of any member of the EU or by the laws of the EU applicable to MOHS to process personal data (**applicable Laws**). Where MOHS is relying on laws of a member of the EU or EU law as the basis for processing personal data, MOHS shall promptly notify the customer of this before performing the processing required by the applicable laws unless those applicable laws prohibit MOHS from so notifying the customer;

- ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the customer, to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

- ensure that all personnel who have access to and/or process personal data are obliged to keep the personal data confidential; and

- not transfer any personal data outside of the European Economic Area unless the prior written consent of the customer has been obtained and the following conditions are fulfilled:

- the transfer is made to a country or an international organisation where the European Commission has decided that the country or international organisation in question ensures an adequate level of protection ("an adequacy decision"); or

- MOHS is processing personal data in a territory which is subject to a current finding by the European Commission under the data protection legislation that the territory provides adequate protection for the privacy rights of individuals; or

- the customer or MOHS has provided appropriate safeguards in relation to the transfer;

- the data subject has enforceable rights and effective legal remedies;

- MOHS complies with its obligations under the data protection legislation by providing an adequate level of protection to any personal data that is transferred; and

- MOHS complies with reasonable instructions notified to it in advance by the customer with respect to the processing of the personal data;

Everyone who works for, or on behalf of, MOHS has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and our internal policy as per their contract of employment.

Our CEO, Helen Hooper, is responsible for reviewing this policy on data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to Helen Hooper and address any written requests to her.

MOHS will process your personal data (including special categories of personal data). We will use your personal data for:

- performing the contract of services between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis on which we intend to rely for processing it.
Examples of how we might process your personal data can be found in the privacy policy. We will only process special categories of your personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent.

If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose to by contacting Helen Hooper.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

7. Sharing your personal data

Sometimes we might share your personal data with group companies or our business partners, contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send your personal data outside the European Economic Area. If this changes, you will be notified of this and the protections which are in place to protect the security of your data will be explained.

8. Data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we will take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we will also notify the Information Commissioner's Office within 72 hours.

9. Subject access request

MOHS will respond to any request from a data subject and ensure compliance with its obligations under the data protection legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.

Data subjects can make a 'subject access request' (SAR) to find out the information we hold about them. This request must be made in writing. If you wish to make such a request, you should forward it immediately to the person responsible for data, Helen Hooper, who will coordinate a response.

We will respond within one month unless the request is complex or numerous in which case the period in which our response can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

10. Your data subject rights

- You have the right to information about what personal data we process, how and on what basis as set out in this policy;

- You have the right to access your own personal data by way of a subject access request (see above);

- You can correct any inaccuracies in your personal data. To do so you should contact the person responsible for data at MOHS;

- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the person responsible for data at MOHS;

- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the person for responsible for data at MOHS;

- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop;

- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month;

- You have the right to be notified of a data security breach concerning your personal data;

- In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the person for responsible for data at MOHS; and

- You have the right to complain to the Information Commissioner's Office (ICO). You can do this by contacting the ICO direct. Their website has further information on your rights and our obligations, plus a helpline.

Document Control

This procedure was approved by Helen Hooper, CEO, and is issued on a version controlled basis under her signature.

Signature: Date: 21/05/18

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Helen Hooper	18/05/2018

Contact details

MOHS Workplace Health: Helen Hooper, data protection officer, helenhooper@mohs.co.uk / 0121 601 4041

Information Commissioner's Office (ICO): www.ico.org.uk