PRIVACY / DATA PROTECTION STATEMENT

This Statement takes account of UK and EU law and conventions and specifically to address the Data Protection Act and General Data Protection Regulations 2018 (GDPR).

OMM is aware of its obligations under the Data Protection legislation and GDPR, endorses this and will apply the revised data protection principles and has undertaken a number of actions to comply. This statement sets out our policy and the actions taken to comply with our statutory, business and ethical requirements.

1. Data Audit

A comprehensive audit of all data held by OMM has been undertaken to identify all individuals where personal data is collected, recorded and processed by the organisation or a contractor acting on behalf of OMM.

The audit covered employees, service users, clients, subscribers, service providers, suppliers and contractors. The audit also identified where data was being kept, in what format, and why the data was being collected and used.

The opportunity was also taken to review the technical and operational security measures in place to prevent or minimise unintentional or malicious access to, or loss of, personal or confidential organisational data. A report is available from an IT specialist setting out the technical safeguards that are in place.

We will undertake an audit of all types of data collection, recording and processing taking place on an annual basis. We will review the reasons for the data being obtained and justify why this should continue or make a decision it will no longer be obtained.

Similarly, we will review the way in which the data is stored and processed to ensure all appropriate safeguards are in place and security/confidentiality measures are effective. We will:-

- Carry out a risk assessment of data systems and act on the results
- Maintain up-to-date security systems (for example, using firewalls and encryption technology)
- Restrict access to personal data to only those who demonstrate that they need it
- Train all OMM staff on data security
- Review data security regularly.

2. Policies, Guidance & Awareness

To underpin compliance with the legislation and GDPR OMM has reviewed and revised its **Data Protection Policy** and has agreed a **Records Management Policy** that sets out the legal framework and timescales for keeping data and best practice with regard to storing data and destroying material when no longer required**.**

Guidance has been issued to partners, staff, managers and clients on Data Protection and their rights and obligations, as well as **Guidance on Data Operational Security** so that everyone operates in a way and follows procedures that safeguards personal data and prevents accidental or malicious disclosure. Should a breach occur, we have a protocol that enables OMM to immediately take action to minimise the impact and to safeguard personal data.
All staff have attended awareness sessions on the GDPR and an external consultancy commissioned to advise us on the implementation of the GDPR and to provide ongoing monitoring and quality assurance input.

Handbooks, employment contract documentation and client terms and conditions have all been revised to include information and guidance on data protection.

Partners and employees who work from home whether on an ad hoc basis, or more generally, have been asked to sign a data protection declaration to say that any personal data in their possession is kept both confidential and secure.

3. Informing individuals and seeking consent (Privacy Notices)

In the main OMM collects, records and processes personal data either to meet statutory obligations or for legitimate business reasons. There is limited personal data being used for which consent is required, and OMM would never pass on personal data to third parties for marketing or selling purposes without consent.

Partners and employees have been informed of what personal data is being held on them by OMM or third parties and have been asked to check the accuracy of the data and been given the opportunity to update their personal data. The reasons why their data is being collected recorded and used has been explained and their new rights outlined. Individual Stakeholders have been given the opportunity to challenge why their data is being kept, how it is being used and who has access to their data.

Specific consent has been obtained from the individuals where there are no legal requirements or legitimate business reason to collect, record and process their data.

Applicants for job vacancies have been informed that their personal data is being collected and recorded as part of our recruitment and selection process and further information will be recorded and used through the process to select and appoint candidates.

Service Users/Clients have been informed of the personal data that is being held on them and why this is required, how it is safeguarded and why personal data might have to be shared with third parties. Service Users also have the same rights as employees and can challenge OMM.

Service Providers are court officials, legal teams, experts used to provide reports or act as witnesses. OMM shares personal data with these providers in order to act on behalf of clients within the legal and courts system. We would not be able to proceed with cases otherwise. OMM has asked these providers to provide evidence of their compliance with the Data Protection Act and GDPR so that we can reassure our clients.

Community Engagement - where personal data is obtained from those attending events, we will have information made available to be given to, or to alert, participants with regard to their rights under data protection and to safeguard their privacy but bearing in mind these are often public events and the media may use personal details for publication in the media including social media.

Suppliers to OMM - in the main, personal data is not held on suppliers by OMM as supplier contact details are usually available in the public domain as part of their business activities. OMM has however informed suppliers of each party's obligations with regard to data protection.

Contractors to OMM - fall into two groups – those providing a time limited service such as building works or maintenance where their contact details will be as per those of Suppliers and then Contractors who are contracted to provide a specific service to the Council such as HR, Health & Safety, Pensions or payroll services.

Those contractors providing a specific service may have access to the personal data of partners and employees.

Where this occurs, OMM in each case we will have verified that the Contractor has a Data Protection and/or Privacy Policy, complies with the principles of the Data Protection Act, has adequate safeguards and security protocols and only uses the personal data for the purpose we have instructed the contractor to provide.

Subscribers - to receive newsletters, updates and notification of events will have had the opportunity to opt out of OMM continuing to record their details for purposes of sending emails or postal communication about OMM services or other information.

4. Website Privacy Policy

A separate policy is published on OMM's website for users of the website.

5. Access to Data

All individuals whose personal data we process have a number of rights under the Act.

The Act gives you the right to know and, in most instances, access a copy of the personal information we hold about you and to correct any of your data. Your right of access can be exercised in accordance with the Act. Any access request may be made in order to understand how and why OMM are holding your data. We may charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive. We are entitled to request sufficient details to assist us in responding to a request.

Employees consent will be obtained where the organisation is making personal data/information available to those who provide services to the organisation (such as HR advisors), regulatory authorities, governmental or quasi-governmental organisations where no legal requirement exists.

Where contractors are used to obtain, record, store or process personal data on behalf of the organisation, that service provider will only be commissioned or have a contract renewed if they

meet data protection quality assurance standards set by us, so that they can demonstrate compliance with the DPA and GDPR.

There may be certain circumstances where a person's consent cannot be obtained or is not legally required. Before releasing personal data to external organisations (including the Police) OMM will seek to obtain legal advice on its obligations and where necessary, ask for a Court Order or a Magistrates Warrant before release of personal information about partners, employees, service users/clients or others.

OMM's policy is to provide copies of all data that the organisation is obliged to disclose within 20 working days of a request being received by the Data Protection Officer.

OMM considers that if a period of less than one year has elapsed since any previous request for access to data was complied with, it is not reasonable to expect us to be obliged to comply with a further request before a year has elapsed unless there are exceptional circumstances.

Where we have requested an employment reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not to be disclosed, it is our policy that it would normally be unreasonable to disclose such a reference to others unless the consent of the person who gave the reference is obtained.

6. Breach of data protection policy or legal requirements

Any suspected or actual breach of data or privacy, whether direct or indirect, malicious or unintentional, will be reported immediately to the Data Protection Officer and the ICO (Information Commissioner's Office) informed where a significant impact is ascertained.

The organisation will implement its **Contingency Plan** in order to immediately protect personal data and resolve the cause of the breach. An independent investigation and report with lessons to be learnt and actions to be taken will be commissioned.

We will consider any serious breach of the policy and data protection rules to be a serious incident and this will be investigated thoroughly and measures taken to remedy the situation and action taken against those felt to be negligent.

7. Protection against detriment

Partners, Employees, and service users/clients will not suffer any detriment, or penalty for challenging the personal data we hold on them or the processes involved, for making subject data access requests or refusing consent to the obtaining, recording or processing of the individual's personal data.

Anyone concerned about the legal status or ethical use of anyone's personal data by the organisation should report this immediately to the Data Protection Officer.

8. Evaluation and review

This Policy will be regularly reviewed by OMM to ensure its effectiveness and compliance with the law and any necessary changes agreed and implemented in consultation with all stakeholders.

9. Data Protection Officer

OMM has appointed **Paul Lockhart**, OMM's Practice Manager to be their **Data Protection Officer** and the role profile for this post will follow the ICO guidance and be enhanced. To give an independent element to the role the DPO will be supported by **PNC (People Network Consultancy)** who will also operate a helpline for any stakeholders with regard to the OMM's implementation of GDPR or who have any queries in relation to their rights under the regulations. PNC will also be involved in the investigation into any breaches.

Any comments or questions about the operation of this Privacy Statement and OMM's policy should be addressed in writing to the Data Protection Officer at OMM. Danbury House, West Street, Leighton Buzzard, Bedfordshire, LU7 1EP.