Data Protection Policy for Sir Robert McAlpine Limited ("SRM")

1. About this policy

1.1. During the course of SRM's (we, our, us) business we collect, store and process personal data about our clients, suppliers, sub-contractors, our employees, visitors to our project sites and premises, visitors to our websites and others. We recognise that the correct and lawful treatment of this data will maintain confidence in us and will provide for successful business operations.

1.2. This policy document outlines our commitment to adopting the correct practices when processing personal data which we collect or is provided to us, to ensure we obtain, handle, process, transfer and store personal data in compliance with legislation (including the Data Protection Act 1998 and the General Data Protection Regulation (679/2016/EU) (the "**legislation**")). Data users are obliged to comply with this policy when processing personal data on our behalf.

1.3. Our Data Protection Champion is responsible for providing advice and guidance to ensure we comply with the legislation and this policy. This post is held by Drew Norman (Tel: +44333 5661946; email: drew.norman@srm.com). Any queries about this policy or concerns as to whether the policy has been complied with should be directed to the Data Protection Champion in the first instance.

2. The meaning of terms used in this policy

2.1. The words and phrases used in this policy have the meanings set out below:

- **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.
- **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
- **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

- **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

- **Data** users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

- **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

- **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

- **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3. Data protection principles

3.1. We are committed to ensuring that when processing personal data, we comply with the eight enforceable principles of good practice. These provide that personal data must be:

- processed fairly and lawfully;

- processed for limited purposes and in an appropriate way;

- adequate, relevant and not excessive for the purpose;

- accurate;

- not kept longer than necessary for the purpose;

- processed in line with data subjects' rights;

- secure; and

- not transferred to people or organisations situated in countries without adequate protection.

4. Fair and lawful processing

4.1. The legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

4.2. For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds provided by the legislation. These include, among other things, the data subject's **consent** to the processing, or that the processing is **necessary for the performance of a contract** with the data subject, for the **compliance with a legal obligation** to which the data controller is subject, or for the **legitimate interest of the data controller** or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

5. Processing for limited purposes

5.1. We will only process personal data for specific purposes. We will notify those purposes to the data subject when the data is first collected or as soon as possible thereafter.

6. Notifying data subjects

6.1. If we collect personal data directly from data subjects, we will inform them about:

- the purpose or purposes for which we intend to process that personal data;
- the types of third parties, if any, with which we will share or to which we will disclose that personal data; and
- the means, if any, with which data subjects can limit our use and disclosure of their personal data.

6.2. If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter if we intend to retain that information.

6.3. We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

7. Adequate, relevant and non-excessive processing

7.1. We only collect personal data to the extent that it is required for the specific purposes notified to the data subject.

8. Accurate data

8.1. We ensure that personal data we hold is accurate and up to date. We check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date data, or data that is no longer required.

9. Timely processing

9.1. We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10. Processing in line with data subject's rights

10.1. We process all personal data in line with data subjects' rights, in particular their right to:

- request access to any data held about them by a data controller (see 14. below);
- prevent the processing of their data for direct-marketing purposes;
- ask to have inaccurate data amended (see 8. above); and
- prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. Data security

11.1. We take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.2. We put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3. We maintain data security by protecting the confidentiality, integrity and availability of personal data, defined as follows:

- **confidentiality** means that only people who are authorised to use the data can access it.
- **integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **availability** means that authorised users should be able to access the data if they need it for authorised purposes.

11.4. Personal data should therefore be stored on our central computer system or departmental secure files instead of individual PCs.

12. Transferring personal data to a country outside the EEA

12.1. We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), if one or more of the following conditions apply:

- the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms; or
- the data subject has given his consent; or
- the transfer is necessary for a reason set out in the legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject; or
- the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or
- the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with
    - respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

12.2. Subject to the requirements in 12.1, personal data may also be processed by staff operating outside the EEA who work for us or one of our suppliers. If this occurs, we scrutinise that supplier's data protection policy and processes.

13. Disclosure and sharing of personal information

13.1. We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries.

13.2. We may also disclose personal data we hold to third parties:

- in the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.
- if we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.
- if we are under a duty to disclose or share a data subject's personal data to comply with a legal obligation, or to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14. Dealing with subject access requests

Data subjects must make a formal request for information we hold about them. This must be made in writing.

15. Changes to this policy

We reserve the right to change this policy at any time.

Policy dated 28 March 2018