DATA PROTECTION POLICY FOR SIR ROBERT MCALPINE LIMITED ("SRM") – 04DDI-1PY-03

1. About this policy

During the course of Sir Robert McAlpine's (we, our, us) business we collect, store and process Personal Data about our clients, suppliers, sub-contractors, our current and former employees, job applicants, 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.

2. Purpose

2.1. This policy document outlines our commitment to adopting the correct practices when processing Personal Data, to ensure we obtain, handle, process, transfer and store Personal Data in compliance with legislation (including the Data Protection Act 2018 and the UK General Data Protection Regulation (the "legislation"). Depending on the purposes for processing there will be times when we act as the Data Controller, Data Processor or Joint Controller. Those processing personal data on behalf of SRM, for which ever purpose are obligated to comply with this policy.

2.2. 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 Andy Black (email data.protection@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.

3. The meaning of terms used in this policy

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

- **Data Subjects** means the individuals to which the Personal Data relates.
- **Personal Data** means data relating to an individual who can be identified (directly or indirectly) from that data. 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** means the people who or organisations which determine the purposes, and the means in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the Act.
- **Data Processors** means any person (other than an employee of the Data Controller) who processes the Personal Data on behalf of the Data Controller and includes any person or organisation that processes Personal Data on our behalf and on our instructions. Data Controllers may include suppliers which handle personal data on our behalf.
- **Processing** means any activity that involves use of the Personal 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** means personal information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), genetics information, biometric information (where used for identification purposes) and information concerning a person's physical or mental health or condition or sexual life or sexual orientation, 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.

4. Data protection principles

We are committed to ensuring that when processing Personal Data, we will comply with the following principles. These principles are that the Personal Data is:

- processed fairly and lawfully;
- processed for a legitimate purpose and not processed in any way which is incompatible with that purpose;
- adequate, relevant and not excessive for the purpose;
- accurate and up to date and reasonable steps are taken to ensure that inaccurate Personal Data is deleted or corrected without delay;
- not kept longer than necessary for the purpose for which the Personal Data is processed; and
- stored securely using appropriate technical and organisational measures and is protected against unauthorised or unlawful processing.

5. Fair and lawful processing

5.1. 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.

5.2. For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds provided by the legislation as determined by the Data Controller. 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.

6. Processing for limited purposes

We will only process Personal Data for specific purposes. We will notify those purposes to the Data Subject when the Personal Data is first collected or as soon as possible thereafter.

7. Notifying Data Subjects

7.1. 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.

7.2. 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.

7.3. We will also inform Data Subjects whose Personal Data we process that we are the Data Controller with regard to that data.

8. Adequate, relevant and non-excessive processing

We only collect Personal Data to the extent that it is required for the specific purposes notified to the Data Subject.

9. Accurate data

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.

10. Timely processing

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.

11. Processing in line with Data Subject's rights

We process all Personal Data in line with Data Subjects' rights, in particular their right to:

- request access to any data held about them (see 15. below);
- prevent the processing of their data for direct-marketing purposes;
- ask to have inaccurate data amended (see 9. above); and
- prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. Data security

12.1. We take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

12.2. 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 they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

12.3. 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.

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

13. Transferring Personal Data to a country outside the EEA

13.1. 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.

13.2. Subject to the requirements in 13.1, 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.

14. Disclosure and sharing of personal information

14.1. We may share Personal Data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, where there is a legitimate need to do so, and this purpose is clearly understood and complies with all our principle set within this document

14.2. 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.

15. Dealing with subject access requests

Data Subjects must make a formal request for information we hold about them. We request that data subjects do so using our established data subject request mechanisms, managed by the Data Protection team.

16. Changes to this policy

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

Title:	Data Protection Policy		
Owner:	Andy Black	Version:	06
Date of last review:	February 2025	Date of next review:	February 2026