24.0 DATA PROTECTION POLICY

24.1 Policy Statement

24.1.1 Everyone has rights with regard to the way in which their Personal Data is handled. During the course of our activities we will collect, store and process Personal Data about our employees, clients, candidates, suppliers and other third parties we communicate with and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

24.1.2 Data users are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

24.2 About This Policy

24.2.1 The types of Personal Data that Rex Procter and Partners ('we') may be required to handle includes information about current, past and prospective staff, suppliers, clients, candidates, and others that we communicate with. The Personal Data, which may be held on paper, on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 as amended, extended, re-enacted or consolidated from time to time (including without limitation the implementation of the General Data Protection Regulation (EU 2016/679) as it forms part of domestic law in the UK by virtue of section 3 of the European Union (Withdrawal) Act 2018) ('Data Protection Legislation').

24.2.2 This policy and any other documents referred to in it sets out the basis on which we will process any Personal Data we collect from Data Subjects, or that is provided to us by Data Subjects or indirectly from other sources.

24.2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

24.2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

24.2.5 The Data Protection Officer is responsible for ensuring compliance with Data Protection Legislation and this policy. That position is held by the Group Business Manager. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Group Business Manager.

24.3 Definition of Data Protection Terms

24.3.1 **Data** is information which is stored electronically, on a computer, in certain paper-based filing systems or forms part of an accessible record.

24.3.2 **Data Breach** means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data or Sensitive data stored or otherwise processed.

24.3.3 **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 Data Protection Legislation. We are the Data Controller of all Personal Data used in our business for our own commercial purposes.

24.3.4 **Data Processors** include any person or organisation that is not a Data user that processes Personal Data on our behalf and on our instructions.

24.3.5 **Data Subjects** all living individuals about whom we process Personal Data.

24.3.6 **Data Users** are those of our employees or representatives 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.

24.3.7 **Personal Data** means data relating to a living individual who can be identified or who are identifiable directly or indirectly from that data (or from that data and other information in our possession). Personal Data can be by reference to a number of indicators such as name, address, date of birth, location data, an online identifier or one or more factors specific to that persons physical, mental, genetic, economic, cultural or social identity.

24.3.8 **Processing** is any activity that involves the use of Personal Data. This includes collecting, recording or holding Personal Data, or carrying out any operation or set of operations on the Personal Data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

24.3.9 **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 sexual orientation, genetic data, biometric data 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, which often requires the express permission of the person concerned.

24.4 Data Protection Principles

24.4.1 Anyone processing Personal Data must comply with the six enforceable principles of good practice. These provide that Personal Data must be:

24.4.1.1 processed fairly and lawfully and in a transparent manner;

24.4.1.2 processed for specified limited purposes;

24.4.1.3 adequate, relevant and not excessive for the purpose;

24.4.1.4 accurate;

24.4.1.5 not kept longer than necessary for the purpose; and

24.4.1.6 **stored securely with appropriate technical and organisational measures.**

24.5 Fair and Lawful Processing

24.5.1 Data Protection 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.

24.5.2 For Personal Data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in Data Protection 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, processing that is necessary to protect the vital interests of a Data Subject or another person, for the legitimate interests of the Data Controller or the party to whom the data is disclosed. When Sensitive Personal Data is being processed more stringent requirements must be met (often express consent will be required). When processing Personal Data as Data Controllers in the course of our business, we will ensure that those requirements are met.

24.6 Processing For Limited Purposes

24.6.1 In the course of our business, we may collect and process the Personal Data set out in the Schedule to this policy. This may include Personal Data we receive directly from a Data Subject (for example when a client or candidate completes one of our online forms or correspondence sent to us by mail, phone, email or otherwise, and data we receive from other sources (including, for example business partners, sub-contractors, credit reference agencies, third party recruitment organisations, industry related websites who advertise our jobs on our behalf and data available in the public domain).

24.6.2 We will only process Personal Data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by Data Protection Legislation. We will notify those purposes to the Data Subject when we first collect the Data or as soon as possible thereafter.

24.7 Notifying Data Subjects

24.7.1 When we collect Personal Data directly from Data Subjects, we will inform them about:

24.7.1.1 our contact details including those of the Data Protection Officer;

24.7.1.2 the purpose or purposes for which we intend to process that Personal Data along with the legal basis for the processing;

24.7.1.3 the types of third parties, if any, with which we will share or to which we will disclose that Personal Data;

24.7.1.4 if we intend to transfer the Personal Data outside the European Economic Area ('**EEA**'), and the appropriate safeguards which will be in place for the data to be transferred;

24.7.1.5 the period for which the Personal Data will be stored, and/or the criteria which will be used to determine that period;

24.7.1.6 whether the provision of Personal Data is part of a statutory or contractual requirement and the consequences of failing to provide the Personal Data (if relevant);

24.7.1.7 the right for the Data Subject to request access to, rectify, erase or restrict the processing of their Personal Data. They also have the right to withdraw consent to processing, the right to request the Personal Data they have supplied to us is transferred to another Data Controller and the right to receive data requested;

24.7.1.8 the right to lodge a complaint with the Information Commissioner's Office ('**ICO**') regarding the processing; and

24.7.1.9 the existence of automated decision-making including profiling.

24.7.1 If we receive Personal Data about a Data Subject from other sources, we will provide the Data Subject with the details of the source, categories of Personal Data to be processed and the information described in clause 7.1 (excluding the information in clause 7.1.6) as soon as possible thereafter.

24.8 Adequate, Relevant and Non-Excessive Processing

We will only collect and process Personal Data to the extent that it is required for the specific purpose notified to the Data Subject.

24.9 Accurate Data

We will ensure that Personal Data we hold is accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

24.10 Timely Processing and Retention

24.10.1 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will retain Data Subjects Personal Data in accordance with the retention periods described in the Schedule.

24.10.2 We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

24.11 Processing In Line with Data Subject's Rights

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

24.11.1.1 request access to any data held about them (see also clause 0);

24.11.1.2 prevent the processing of their data for direct-marketing purposes;

24.11.1.3 prevent processing on an automated processing basis;

24.11.1.4 have inaccurate or incomplete data amended (see also clause 0);

24.11.1.5 have data erased;

24.11.1.6 restrict processing of Personal Data for limited purposes;

24.11.1.7 have copies of their Personal Data sent to them in a commonly used format and transferred to another Data Controller (see clause 16 for further details when this right applies);

24.11.1.8 have details of their Personal Data sent to them in an electronic or other commonly used format (see also clause 16); and

24.11.1.9 prevent processing that is likely to cause damage or distress to themselves or anyone else.

24.11.1 Where Data Subjects contact us to exercise the above rights these will need to be passed to the Data Protection Officer as soon as possible. Where Personal Data has been shared with third parties, we must notify such third parties that the Data Subject has exercised these rights.

24.12 Data Security

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

24.12.2 We will 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.

24.12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the 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. Personal Data should therefore be stored on our central computer system instead of individual PCs.

24.12.4 Security procedures include:

Entry controls. Any stranger seen in entry-controlled areas should be reported.

Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

Methods of disposal. Paper documents with confidential information on should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended.

24.13 Data Breaches

24.13.1 Where a Data Breach occurs staff should inform the Data Protection Officer immediately (or where this is not possible no later than 48 hours after discovering the breach) to enable the Data Protection Officer to take remedial action as soon as possible.

24.13.2 It will be necessary for the breach to be reported to the ICO within 72 hours of discovering the breach where there the breach is likely to result in a risk to the rights and freedoms of individuals or if unresolved, likely to have a significant detrimental effect on the individual (e.g. discrimination, damage to reputation, financial loss, confidentiality or other significant or social disadvantage). It will also be necessary to inform the Data Subject where a serious breach occurs which is likely to be a high risk to the rights and freedoms of the Data Subject. The Data Protection Officer will be responsible for reporting such breaches.

24.13.3 Where we act as Data Processor for a third party, we must make the Data Controller aware of the breach as soon as possible.

24.14 Transferring Personal Data to a Country Outside The EEA

24.14.1 We may transfer Personal Data we hold to a country outside the EEA, provided we have notified the Data Subject and one of the following conditions applies:

24.14.1.1 the country to which the Personal Data are transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms as determined by the European Commission; or

24.14.1.2 Personal Data is transferred using appropriate safeguards approved by the European Commission or the ICO.

24.15 Disclosure and Sharing Of Personal Information

24.15.1 We are required to comply with obligations under Data Protection Legislation where we use third parties to process Personal Data on our behalf. In these circumstances, such parties will be acting as our Data Processor and the Data Protection Legislation requires us to put in place a contract in writing with each of our Data Processors which

contain a number of provisions to help safeguard the Personal Data. If you are responsible for the drafting or negotiation of contracts with Data Processors, you must seek further advice from the Data Protection Officer to ensure the contracts contain all necessary data protection provisions.

24.15.2 Where we share Personal Data with third parties for their own use (and they will not be processing data on our behalf) it will be necessary to enter into a data sharing agreement. We need to ensure that such agreements contain certain provisions such as the third party will only process the Personal Data for certain purposes, to return the Personal Data to us in certain circumstances and have adequate security measures in place.

24.15.3 We may also disclose Personal Data we hold to third parties:

24.15.3.1 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.

24.15.3.2 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.

24.15.4 If we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation.

24.15.5 We may also share Personal Data we hold with selected third parties for the purposes set out in the Schedule.

24.16 Dealing with Subject Access Requests

24.16.1 **Data Subjects may ask for details regarding the information we hold about them. The request will typically be in writing but may be made orally (e.g. during a telephone call). Requests may be clearly signposted as a 'data subject access request', or make reference to the GDPR, data protection or personal data, but they do not need to do so to be a valid request. Any request for the data we hold about a data subject will be treated as a subject access request. Employees who receive a request should forward it to the Data Protection Officer immediately to enable a response to be provided within the statutory one month deadline, although this can be extended by up to a further 2 months in the event the request is complex. In the event that it is necessary to extend the deadline we will inform you of this fact and of the reasons for this.**

24.16.2 Subject to meeting the conditions in clauses 16.2.1 and 16.2.2 and upon request, we must send a Data Subject copies of their Personal Data in an electronic or other commonly used format and/or transfer the Personal Data to another Data Controller. These rights are exercisable where:

24.16.2.1 the Personal Data is processed electronically; and

24.16.2.2 the processing of the Personal Data is based upon the Data Subject's consent or where the processing is necessary for the performance of a contract.

24.16.3 We cannot charge the Data Subject a flat fee for complying with a request. We can refuse to respond to a request or charge a reasonable fee where a request is

manifestly unfounded or excessive. A reasonable administrative fee may also be charged where further copies of data are requested.

24.16.4 Refer to the Data Protection Officer in difficult situations. Employees should not be bullied into disclosing personal information.

24.17 Internal Records

24.17.1 We are required to keep records of our processing activities. Employees will assist the Data Protection Officer to ensure such records are collated and updated. (To the extent not covered within the Schedule) such records must include details of:

24.17.1.1 the individual currently appointed as the data protection officer;

24.17.1.2 the categories of Data Subjects and Personal Data;

24.17.1.3 the purpose of the processing;

24.17.1.4 any transfer of Personal Data to parties outside the EEA and the safeguards put in place to protect the transfer of such Personal Data;

24.17.1.5 where possible, the retention periods for different types of Personal Data;

24.17.1.6 where possible, a general description of the technical and organisational security measures we have in place to protect Personal Data; and

24.17.1.7 a record of Data Breaches including details of the breach, its effects and remedial action taken.

24.18 Data Breaches

24.18.1 A data breach may take many forms for example:

24.18.1.1 loss or theft of data or equipment on which personal information is stored;
24.18.1.2 unauthorised access to or use of personal information either by a member of staff or third party;
24.18.1.3 Loss of data resulting from an equipment or systems failure;
24.18.1.4 Human error, such as accidental deletion or alteration of data;
24.18.1.5 Unforeseen circumstances, such as fire or flood;
24.18.1.6 Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
24.18.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

24.18.2 We will:

24.18.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
24.18.2.2 notify the affected individuals if the data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

24.19 Changes to this Policy

24.19.1 We reserve the right to change this policy at any time. Where appropriate, we will notify you of these changes by mail or email.

Alex Blenard
Executive Director

Date: March 2025

Schedule
Data processing activities

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Type of recipient to whom Personal Data is transferred	Transfer of data outside EEA and safeguards in place to protect data	Retention period
Employment records (including job application, C.V, references, details of disciplinary action taken, attendance and length of service, contract of employment, pension scheme number), bank details	Employee	Collecting, maintaining and using employee information	Payroll, disciplinary, health & safety and statutory reasons.	HMRC, DWP, Pension Scheme, Insurance Schemes, References, Banks		Throughout employment and for 3 years after employee ceases employment. For unsuccessful applicants that apply for a position with us we will retain data for a period of 2 years.
Client name, contact address, email address, telephone numbers, individual addresses, individual mobile numbers	Client	Maintaining client information	Administration of projects.	Internally RPP and third parties in relation to each specific project		Throughout the duration of the project and / or business relationship.

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Type of recipient to whom Personal Data is transferred	Transfer of data outside EEA and safeguards in place to protect data	Retention period
Candidate information for potential applicants for vacancies or speculative enquiries	Candidate	Collecting and maintaining candidate information	Interviewing for vacancies	Internally RPP		For unsuccessful applicants that apply for a position with us we will retain data for a period of 2 years.
Supplier name, contact address, email address, telephone/mobile number, bank details, insurance cover.	Supplier	Maintaining office supplies	Facilities / office / fleet management	Internally RPP, insurance companies, banks		Throughout the duration of the order and / or business relationship.