DATA PROTECTION POLICY

1. INTRODUCTION

1.1 Wates Group Limited ("Wates", "we", "our", and "us") is a family-owned Construction, House Building, Maintenance, Building Services, Facility Management and Managed Office Services company. As a leader in our chosen markets, our objective is to deliver excellent services for our customers, resulting in safe, fair and professional contracting services at all times.

1.2 In order to provide our services, we are required to collect, process, use and retain certain personal data for a variety of business purposes. We also process the personal data of visitors to our website, job applicants, any individual who signs up to receive our business email notifications, the data of our employees, and we may process the personal data of representatives of our clients in connection with the provision of our services.

1.3 Our approach to data protection is one of sensible risk management which is driven by our Guiding Framework:

2. ABOUT THE POLICY

2.1 This Policy sets out what we expect from you in order for us to comply with applicable Data Protection Laws (as defined below). Your compliance with this Policy and all related policies and guidelines is mandatory. Any breach of this Policy may result in disciplinary action.

2.2 This Policy describes how personal data must be collected, handled and stored to meet the company's data protection standards and to comply with all applicable laws and regulations relating to processing of personal data and privacy, including without limitation the General Data Protection Regulation ("**GDPR**") and any other applicable data protection legislation in force from time to time and including where applicable the guidance and codes of practice issued by the Information Commissioner or any other relevant regulator ("**Data Protection Laws**").

2.3 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 other sources.

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

2.5 The Privacy Team is responsible for ensuring compliance with applicable Data Protection Laws and with this Policy. 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 Privacy Team at GDPR@wates.co.uk or the Data Protection Manager.

3. DEFINITIONS OF DATA PROTECTION TERMS

"**Data controller**" or "**controller**" means the organisation that determines the purposes and means of the processing of personal data. Wates is the controller of all personal data used in our business for our own commercial purposes.

"**Personal data breach**" or "**breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"**Data processor**" or "**processor**" means an organisation or individual which processes personal data on behalf of Wates. Employees of controllers are excluded from this definition but it could include suppliers which handle personal data on Wates's behalf.

"**Data subjects**" for the purpose of this Policy means all living individuals about whom Wates holds personal data for example, including staff, customers, suppliers, job applicants, business- to-business contacts and consumers. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

"**Personal data**" means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified,

directly or indirectly, in particular by reference to an identifier such as a name, an identification number (NI number), location data, online identifier (IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

"**Processing**" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Sensitive personal data**" or "**special categories of personal data**" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data (e.g. DNA, finger prints etc.). Please however note that criminal records data is dealt with separately under Article 10 of the GDPR.

"**The consent of the data subject**" means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

4. SCOPE OF POLICY

4.1 The Policy applies to personal data in all its forms whether on paper or stored electronically. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of applicable Data Protection Laws or our contractual obligations.

4.2 With regard to electronic systems, the Policy applies to use of Wates equipment and privately/externally owned systems when connected to our network, including but not limited to databases, emails and CCTV.

4.3 The Policy applies to all company owned/licensed data and software.

5. OBJECTIVES OF POLICY

The Policy will ensure that Wates:

5.1 Complies with applicable Data Protection Laws and follows good practice;

5.2 Protects the rights of its staff, customers, clients and suppliers;

5.3 Is transparent about how it stores and processes personal data; and

5.4 Protects itself from the risks of a data breach or other unlawful processing of personal data.

6. DATA PROTECTION LAWS

6.1 Applicable Data Protection Laws describe how organisations must collect, handle and store personal data and these rules apply regardless of whether data is stored electronically or in paper format.

6.2 Anyone processing personal data must comply with the principles set out in the GDPR, that personal data must:

6.2.1 Be processed fairly and lawfully (lawfulness, fairness and transparency);

6.2.2 Be collected only for specific and lawful purposes and not processed in a manner that is incompatible with those purposes (purpose limitation);

6.2.3 Be adequate, relevant and limited to what is necessary for the purposes for which it was collected (data minimisation);

6.2.4 Be accurate and kept up to date (accuracy);

6.2.5 Not be held for longer than is necessary for the purposes for which it was collected (storage limitation);

6.2.6 Be processed in accordance with the data subject's rights;

6.2.7 Be processed in a manner that ensures appropriate security (integrity and confidentiality); and

6.2.8 Not be transferred to a country or a territory outside the European Economic Area ("**EEA**") unless that country or territory ensures an adequate level of protection.

6.3 Where we process personal data we are responsible for demonstrating compliance (accountability) with the principles set out in section 6.2 above.

7. RESPONSIBILITIES

7.1 Whilst Wates is ultimately responsible for ensuring that Wates meets its legal obligations under applicable Data Protection Laws, you are responsible for compliance with this Policy. Our employees are collectively and personally responsible for the communication, understanding and practical application of this policy. This policy will be made available to all new employees at recruitment stage and to our supply chain and to any other interested parties upon request. Revisions will be communicated to those affected by the changes.

7.2 The Privacy Team is responsible for:

7.2.1 Ensuring all systems, services and equipment used for storing data meet acceptable security standards;

7.2.2 Performing regular checks and scans to ensure security hardware and software is functioning properly;

7.2.3 Evaluating any third-party services the company is considering using to store or process data;

7.2.4 Carrying out periodic risk assessments and establishing and maintaining effective contingency plans;

7.2.5 Regular reviews of this Policy; and

7.2.6 Regular reviews of the Information and Data Security Policy and monitoring of staff compliance with such policy.

7.3 All Wates staff are responsible for:

7.3.1 Keeping all personal as well as business critical and potentially sensitive data secure by taking sensible precautions and following the guidelines in this Policy;

7.3.2 Informing the Privacy Team immediately about data breaches or potential data breaches, and any perceived risks or issues in relation to data security in particular any observed or suspected breach of this Policy;

7.3.3 Requesting guidance from the Privacy Team if unsure of any aspect of data protection;

7.3.4 Keeping updated about data protection risks and issues;

7.3.5 Reviewing and updating all data protection procedures and related policies, in line with legal requirements;

7.3.6 Attending regular data protection training;

7.3.7 Referring requests received from data subjects exercising their rights under applicable Data Protection Laws (see section 12 'Processing in line with Data Subject's Rights' below) to the Privacy Team immediately;

7.3.8 Checking and approving any contracts or agreements with third parties that may handle the company's personal data, or referring them to Group Legal; and

7.3.9 Complying with the Information and Data Security Policy.

7.4 The Executive Committee has overall responsibility for ensuring this policy is complied with and will review it at least once per year, and at such other times as may be required, to ensure it remains relevant and appropriate to the aims and objectives of our business.

8. FAIR AND LAWFUL PROCESSING

8.1 Data Protection Laws are 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.

8.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out under applicable Data Protection Laws. 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.

8.3 We generally process personal data during the course of our business on the basis that the processing is necessary for the performance of a contract with the data subject (whether this be our employee or customer). To the extent the processing of personal data is necessary for staff administration and efficiency purposes, provided that such processing is not to the detriment of our employees; we process personal data on the basis that is it is in our legitimate interests. Any personal data we process in the course of our business

marketing is also on the basis of our legitimate interests, provided it is not to the detriment of the data subject.

8.4 Our privacy policies explain the legal basis on which we process personal data; these are available on request. A version of our Data Protection Notice for our clients and customers is available on our website.

9. PROCESSING FOR LIMITED PURPOSES

9.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes, and it cannot be used for new, different or incompatible purposes from that disclosed when it was first obtained, unless you have informed the data subject of the new purposes, and they have consented (if necessary).

9.2 We will only process personal data for purposes specifically permitted by applicable Data Protection Laws. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter, and such purposes may include (amongst others):

9.2.1 Providing information to our clients and customers;

9.2.2 Fulfilling our contractual obligations to our employees;

9.2.3 Compliance with our legal, regulatory and corporate governance obligations and good practice;

9.2.4 Marketing our business; and

9.2.5 Improving our services.

10. PROVIDING INFORMATION

10.1 In the course of our business, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by an individual subscribing to our email notification service, or by an employee providing bank details for remuneration purposes) and data we receive from other sources (for example, sub-contractors providing us with technical website services).

10.2 If we collect personal data directly from data subjects, we shall ensure that data subjects are aware that their data is being processed, and that they understand:

10.2.1 The purpose of the processing and the lawful basis for the processing;

10.2.2 The legitimate interests of Wates or third party, where applicable;

10.2.3 Any recipient or recipients of their personal data;

10.2.4 Details of transfers to third country and safeguards;

10.2.5 Retention periods or criteria used to determine the retention periods;

10.2.6 The existence of each of the data subject's rights;

10.2.7 The right to withdraw consent at any time, where relevant;

10.2.8 The right to lodge a complaint with a regulator.

10.2.9 Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.

10.2.10 The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

10.3 If we collect personal data from a third party about a data subject, we will provide the data subject with the above information as soon as possible, and provide any additional information as prescribed by applicable Data Protection Laws.

10.4 To assist with our compliance of the above requirements, we have privacy statements setting out how we use personal data relating to data subjects (see section 8.4 above).

11. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

We will only collect personal data to the extent that it is necessary in relation to the purposes for which they are processed. As such, we will not process personal data obtained for one purpose for any unconnected purpose unless the data subject concerned has agreed to this or would otherwise reasonably expect this.

12. DATA ACCURACY

12.1 If we receive a request to update or correct any personal data we hold, and provided we have authenticated the identity of the data subject in question, we will take all reasonable steps to ensure that personal data we hold is accurate and

kept up to date. We will take all reasonable steps to destroy or amend inaccurate, incomplete or out-of-date data.

12.2 It is the responsibility of all staff to take reasonable steps to ensure that personal data is kept as accurate and up to date as possible and personal data should be updated as inaccuracies are discovered. For example, if an e-mail address is no longer in service, it should be removed from the database.

12.3 Data subjects may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Privacy Team promptly.

13. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

13.1 We will process all personal data in line with data subjects' rights to and in connection with their personal data in accordance with the Data Protection Laws.

13.2 If a data subject makes a request (written or otherwise) to exercise any right (or purported right) in respect of their personal data, you should immediately forward it to the Privacy Team. Employees should not in any circumstances be bullied into disclosing personal information.

13.3 The Privacy Team will handle the response to the request and ensure that the identity of anyone making a request has been adequately verified before handing over any information.

13.4 Any complaints received from a data subject should be escalated to the Privacy Team.

14. DATA RETENTION

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. For more information please see our Data Retention Policy.

15. DATA SECURITY

15.1 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. We will put in place procedures and technologies appropriate to our size, scope and business, our available resources and the amount of personal data that we process. These measures will maintain the security of all personal data from the point of collection to the point of destruction. We will regularly evaluate and test the effectiveness of these measures to ensure security of our processing of personal data in accordance with our Information and Data Security Policy.

15.2 We will only use data processors that agree to comply with these procedures and policies, or if they put in place adequate measures their self. We will conduct adequate due diligence on all data processors and take all steps required by any applicable Data Protection Laws where we appoint a data processor, including ensuring such data processor:

15.2.1 enters a written agreement with Wates that includes sufficient guarantees as to the security measures the data processor has in place;

15.2.2 imposes confidentiality obligations on all personnel who process the relevant data;

15.2.3 ensures the security of the personal data that it processes;

15.2.4 provides Wates with all information necessary to demonstrate compliance with applicable Data Protection Laws;

15.2.5 either returns or destroys the personal data at the end of the relationship;

15.2.6 implements measures to assist Wates in complying with the rights of data subjects; and

15.2.7 continues to comply with its data protection obligations when processing personal data (i.e. by monitoring its compliance).

15.3 In addition, where we use data processors we will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those data processors to ensure that such data processors' data protection obligations are of an equivalent standard to Wates's.

15.4 Where appropriate, we will review the activities and processes of processors we use to check that they are processing personal data in line with our requirements and the requirements of the Data Protection Laws, and ensure that the processor confirms they regularly test their security measures to ensure they meet the applicable standards.

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

15.5.1 **Confidentiality** means that only people who are authorised to use the data can access it.

15.5.2 **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

15.5.3 **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 Wates's central computer system instead of individual PCs.

15.6 Security procedures include (but are not limited to):

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

15.6.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information may be considered confidential and sensitive). Where personal data is stored in desks and cupboards, these should only be accessible by individuals whom are authorised to access such personal data (e.g. personal data should not be stored in communal cupboards / drawers that are accessible by all staff).

15.6.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

15.6.4 **IT Security.** You must comply with our Information and Data Security Policy, CCTV Policy, Biometric Rules, and any other relevant policies at all times when handling personal data.

15.6.5 **Privacy by design and default.** Privacy by design is an approach to future Wates projects that promotes privacy and data protection compliance from the start. This may involve the person responsible for the project conducting a data protection impact assessment (also known as data privacy impact assessments or "DPIAs") prior to the start of any project that involves the processing of personal data. DPIAs are a tool which can help us identify the most effective way to comply with our data protection obligations and meet data subjects' expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. DPIAs are required when we are using new technologies, and when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals (such as the processing of sensitive personal data or systematic monitoring of public areas (e.g. CCTV)).

15.7 It is your responsibility to ensure that you keep personal data secure against loss or misuse in accordance with this Policy.

16. SHARING PERSONAL DATA

16.1 If we share personal data with third parties, we will do so in line with applicable Data Protection Laws. We may have to share personal data with government bodies, such as HMRC, our legal advisers, our insurers, a prospective employer, the police and any appropriate court or government department from time to time as required. In addition, we share personal data with third parties such as payroll providers, outsourced IT providers, phone providers, immigration lawyers, psychometric test providers, and criminal background check agencies.

16.2 You may only share the personal data we hold with another employee, agent or representative of our group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions (see section 18 below).

16.3 You may only share the personal data we hold with third parties if:

16.3.1 sharing the personal data complies with the Data Protection Notice provided to the data subject, and, the data subject's consent has been obtained or other legal basis for processing has been established;

16.3.2 the data sharing complies with any applicable cross-border transfer restrictions.

17. DATA STORAGE

17.1 Personal data should be stored only electronically whenever possible and the recording of personal data in paper format should be kept to a minimum. In exceptional circumstances where personal data is recorded in paper format, it should be kept in a secure place to prevent unauthorised access to such personal data by unauthorised personnel.

17.2 When you store personal data, whether electronically or in paper form, you must protect it from unauthorised access, accidental deletion and malicious hacking attempts in accordance with our Information and Data Security Policy.

18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

18.1 We may transfer personal data we hold to a country outside the EEA, such as the United States of America, provided that one of the following conditions applies:

18.1.1 The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

18.1.2 The data subject has given his/her explicit consent (having been properly informed (i.e. of the risks etc.)).

18.1.3 The transfer is necessary for one of the reasons set out in any applicable Data Protection Laws, including: the performance of a contract between us and the data subject (or a third party (provided it is in the interests of the data subject)); or to protect the vital interests of the data subject.

18.1.4 The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

18.1.5 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.

18.2 You should not transfer personal data outside the EEA without first discussing it with the Privacy Team.

19. MARKETING

19.1 We are subject to certain rules and privacy laws when marketing to our customers.

19.2 For example, a data subject's prior consent may be required for unsolicited direct marketing by electronic means.

19.3 A data subject's objection to direct marketing must be promptly honoured. If a subscriber opts out of receiving email notifications at any time, their details must be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

19.4 You must comply with Wates's guidelines on direct marketing to customers.

20. DATA BREACHES

20.1 If you suspect or become aware of any unauthorised or unlawful processing, or accidental loss or destruction of, or damage to, any Wates personal data, they must report this to the Privacy Team immediately. Examples include:

20.1.1 Hardware loss or theft (e.g. losing an electronic device such as a smartphone, tablet or laptop containing Wates personal data);

20.1.2 Unauthorised or unlawful access to Wates personal data held electronically or physically (e.g. an intruder to the building accessing paper documents or a system being 'hacked'); and

20.1.3 Inadvertent disclosure (e.g. an employee accidentally disclosing a marketing list of email addresses to a third party).

20.2 Data breaches involving IT equipment or electronic data must be reported to the Privacy Team immediately. The Privacy Team will work with relevant staff, including the IT team, to make sure data is secured and that any risks associated with the breach are minimised.

20.3 Where personal data has been lost or stolen, the Privacy Team will (if required under applicable Data Protection Laws) ensure that the ICO is notified and that all reasonable steps are taken to inform any affected data subjects. Unless specifically authorised to do so, you should not attempt to notify the ICO and/or data subjects. If you become aware of or suspect that a data breach has occurred, you should immediately

escalate the matter to a supervisor and the Privacy Team in accordance with this Policy. You must preserve all evidence relating to the potential data breach.

20.4 Unlawful use of data is a criminal offence under data protection laws and may be subject to sanctions. Breaches of this policy and Data Protection Laws will be dealt with under the Wates Group's disciplinary procedures, and may lead to dismissal. Any unauthorised use of corporate email by staff, including the sending of sensitive or personal data to unauthorised persons, or the use of such data that brings Wates into disrepute will be regarded as a breach of this policy.

21. DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the applicable Data Protection Laws allow personal data to be disclosed to law enforcement agencies without the knowledge of the data subject. Under these circumstances Wates will disclose requested data. However the Privacy Team will check that the request is legitimate seeking assistance from the company's legal advisers where necessary.

22. POLICY AWARENESS

22.1 The Policy will be made available to all staff. Staff and authorised third parties given access to Wates personal data will be advised of the existence of Wates's relevant policies, codes of conduct and guidelines that relate to the processing of personal data.

22.2 Training will be given to all staff when they first join Wates. Additional training will also be provided on a periodic basis as necessary to refresh your knowledge or where there has been a substantial change in the Data Protection Laws or this Policy, to ensure all staff are aware of their obligations under this Policy and applicable Data Protection Laws.

22.3 It is compulsory that you complete this training.

22.4 You are obliged to comply with this Policy when processing personal data on behalf of us. Any breach of this Policy may result in disciplinary action.

23. CHANGES TO THIS POLICY

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

24. QUESTIONS

Please refer questions to the Privacy Team at gdpr@wates.co.uk or Wates' Data Protection Manager.

For and on behalf of the Executive Committee
DAVID ALLEN
Chief Executive, July 2019