

DATA PROTECTION POLICY



Wates Group is a family owned Construction, House Building, Maintenance, Building Services and Facility Management 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.

We recognise that in order to carry out our services, Wates must collect and use personal data relating to the people with whom and for whom it works. 'Personal data' means any information relating to a living individual from which that individual may be identified (including, for example, their name, address or payroll number), whether by itself or taken together with other information in the possession of the Wates Group. It includes any expression of opinion about the individual and any indication of the individual's intentions. 'Individuals' may include members of the public, current, past and prospective employees, clients, customers, suppliers and sub-contractors.

We will manage any personal data in accordance with the Data Protection Act 1998 and other related legislation, in whichever manner that such data is collected, recorded or used (whether on paper, databases, emails, CCTV or telephone records, or recorded by any other means). Wates follows the eight data protection principles set out in the Data Protection Act 1998, and understands its obligations to ensure that personal data is managed fairly, lawfully, accurately and securely. These principles require that personal data shall:

- be processed fairly and lawfully
- be processed for limited purposes
- be adequate, relevant and not excessive
- be accurate and up-to-date
- not be kept for longer than is necessary
- be processed in line with the rights of data subjects
- be processed securely
- not be transferred to a country or territory outside the European Economic Area without adequate safeguards

Our approach to data protection is one of sensible risk management which is driven by our core values as listed below:

INTEGRITY: We do not compromise our integrity. We manage the personal data relating to the people for whom, and with whom we work, lawfully and fairly. Our relationships are built on trust and our reputation matters to us.

INTELLIGENCE: We take an intelligent approach to how we deal with personal data.

TEAMWORK: Our people and processes work together to ensure our continued success in developing, implementing and maintaining our strategy on data protection.

PERFORMANCE: We work hard to generate excellent results in order to achieve the highest standards in data protection.

RESPECT FOR PEOPLE AND COMMUNITIES: We strive for an inclusive culture based upon mutual respect. We respect each other, our suppliers, our customers, our partners, our communities and society at large and value their data security.

In particular, in compliance with the Data Protection Act 1998 and all related legislation, we will:

- develop, implement and review our data protection strategies on a regular basis
- use Closed Circuit Television (CCTV) only where it is a necessary and proportionate way of managing an issue, and ensure that signs are prominently displayed to make clear that CCTV is in use
- put in place appropriate technical, training, organisational, administrative and security procedures for the:
 - * collection, processing, management and security of personal data
 - * management of any request for access to personal data (including CCTV footage) made by an individual
 - * obtaining where necessary the consent of those to whom any personal data belongs before the release of such data

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.

Our employees have a personal responsibility to report any actual, near miss, or suspected data breaches to the Wates Group Commercial Legal Advisor (who is the Wates Group's Data Protection Officer) for investigation. Breaches of his policy will be dealt with under the Wates Group's disciplinary procedures, and could lead to dismissal in appropriate circumstances. 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.

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.

For and on behalf of the Executive Committee

DAVID ALLEN
Acting Chief Executive
November 2017