Balfour Beatty respects the privacy of all individuals and takes very seriously its responsibilities under the Data Protection Act 1998 (“DPA”). This policy is designed to ensure that all information held on individuals is properly handled in all cases.

The DPA requires that the “personal data” of living individuals that is kept by Balfour Beatty plc and its UK operating companies on computer or well structured paper files must be “processed” in accordance with eight principles (which are described in Table A).

Personal data is defined very widely and is any data from which a living individual can be identified either from the information alone, or with other information which is in (or likely to come into) the possession of the UK operating company. Examples of personal data include names, addresses, and photographs, CCTV images of individuals, salary/job titles or opinions which allow individuals to be identified. Personal data also includes “sensitive personal data” – this is information about an individual’s racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life or criminal offences/proceedings.

“Individuals” could be any living person – for example, employees, agency staff, customers, contractors, suppliers and job applicants.

 “Processing” includes obtaining, recording, holding, using, disclosing or erasing the personal data. In effect almost any activity involving personal data will fall within the scope of the DPA.

Balfour Beatty’s policy is to comply with the DPA and it does not condone anyone processing personal data inappropriately on its behalf. Any breach by Balfour Beatty or any of its UK operating companies of the DPA may lead to fines and/or enforcement action being taken against Balfour Beatty and/or a UK operating company by the Information Commissioner (the body that enforces compliance with the DPA). Of equal concern is that any breach may attract media scrutiny and may lead to a potentially adverse impact on our reputation.

 This policy applies to all UK operating companies and all staff working within them (including employees, agency workers, contractors and temporary staff) who may process personal data about employees or other individuals. Compliance with this policy is mandatory.

 The Managing Director (or his/her delegate) for each UK operating company has the responsibility for establishing and implementing effective practices and procedures across it to give effect to this policy. When implementing this policy, UK operating companies may find the separate document: Implementation of Balfour Beatty UK Data Protection Policy: General Guidance useful.