

SCOPE

This policy applies to all Employees.

This policy supplements the Company's other policies relating to data protection, acceptable use, CCTV recording, drug and alcohol, and retention.

Separate privacy policies may apply to the processing of separate types of data in specific circumstances. If this is the case, these policies will be communicated to the relevant Employees.

This policy does not form part of your contract of employment. The Company may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to Employees and published on the BMS.

PURPOSE

The Company values the privacy of our Employees. This policy sets out in more detail our practices in relation to the collection and use of your personal data.

ABBREVIATIONS / DEFINITIONS

Business Purposes	means the purposes for which personal data may be used by the Company, e.g. personnel, administrative, financial, regulatory, payroll, security and business development purposes
Company	means Balfour Beatty Group Employment Limited;
Personal Data	means information relating to a living individual, such as job applicants, current and former employees, agency, contract and other Employees, clients, suppliers and marketing contacts who can be identified from that data or from that data and other information which the Company has or is likely to have. This can include name, address, email address, financial information, CCTV images, MAC and IP addresses, location data, aliases, preferences and profiles, amongst other things
Processing Data	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Sensitive personal data/ special categories	means personal data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data for the purpose of uniquely identify a person, data concerning physical or mental health or condition, sexual life, criminal offences, or related proceedings. Any use of sensitive personal data must be strictly controlled in accordance with this policy
Employees	means all directors, consultants, employees, interns, volunteers and temporary Employees of the Company
Supervisory Authority	means the independent regulatory body responsible for monitoring the application of data protection law in its jurisdiction. The Information Commissioner is the Supervisory Authority for the Company.

PROCEDURAL REQUIREMENTS

1. Introduction

- 1.1 The controller of your personal data is the Company, being your employer as set out in your employment contract / terms of employment. Speak to the relevant Data Protection Officer for your business unit immediately if you are unsure who the data controller of your information is.

The Data Protection Officer with ultimate responsibility for ensuring the application of this policy is Matthew Kay, Group Data Protection Officer. There are also a number of other Data Protection Officers across the Company's various business units. Their names and contact details are set out in Appendix 1 at the end of this document.

- 1.2 The Company processes your personal data in order to discharge its obligations as an employer. It does so for the Company's own legitimate interests (except as otherwise set out in this policy and provided that legitimate interest does not override your right to privacy), to fulfil its contract with you and in order to comply with any applicable legal obligation.

On occasion, the company may also process your personal data in accordance with paragraph 3.4.

- 1.3 The legitimate interests referred to in paragraph 1.2 are as follows:
- the Company's ability to manage its workforce and ensure employees are behaving appropriately; and
 - the profitability, sustainability, success, reputation and development of the Company's business.
- 1.4 In the event that arrangements or purposes for the processing of your personal data are to be materially revised, the Company shall issue an updated version of this policy, or a supplement to it, to inform you of the proposed changes.
- 1.5 Your personal data will only be processed in accordance with data protection law and regulation and for the purposes set out in paragraph 1.2 and the Company will not process your personal data in any manner incompatible with those purposes unless we are required by law to do so. The Company will also endeavour to comply with the Information Commissioner's code of practice on the use of personal data in employee/employer relationships.

2. Collection of Personal Data

- 2.1 Your personal data will only be processed in accordance with data protection law and regulation and for the purposes set out in paragraph 1.2. The Company will not process your personal data in any manner incompatible with those purposes unless we are required by law to do so. Most often, we will use your personal information to perform the contract we have entered into with you, to comply with a legal obligation and where it is necessary for our legitimate interests and your right to privacy does not override those interests. If the Company needs to process your sensitive personal data, we will only do so where paragraph 2.3 also applies.
- 2.2 The Company holds and processes the personal data of Employees, including:
- 2.2.1 Name, address and contact details, including email address and telephone number, date of birth and gender;
- 2.2.2 The terms and conditions of employment;
- 2.2.3 Details of qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;

- 2.2.4 Information about remuneration, including entitlement to benefits such as pensions or insurance cover;
 - 2.2.5 Details of bank accounts and national insurance numbers;
 - 2.2.6 Information about marital status, next of kin, dependants and emergency contacts;
 - 2.2.7 Information about nationality and entitlement to work in the UK
 - 2.2.8 Information about criminal records;
 - 2.2.9 Details of days of work and working hours including attendance at work;
 - 2.2.10 Details of periods of leave taken, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
 - 2.2.11 Details of any disciplinary or grievance procedures, including any warnings issued to you and related correspondence;
 - 2.2.12 Assessments of performance, including appraisals, performance reviews and ratings, training they have participated in, performance improvement plans and related correspondence;
 - 2.2.13 Information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
 - 2.2.14 Details of trade union membership; and
 - 2.2.15 Equal opportunities monitoring information, including information about ethnic origin, sexual orientation, health and religion or belief.
- 2.3 Sensitive personal data/special categories of data require a higher level of protection. Most often we may process this special category of data where:
- 2.3.1 we need to carry out our legal obligations or exercise rights in connection with employment;
 - 2.3.2 we need to establish, exercise, or defend a legal claim;
 - 2.3.3 where the processing is necessary for the assessment of your working capacity, occupational health, obtaining a medical diagnosis (including fitness for work general practitioner doctor notes and sickness notes) or where it is needed in the public interest (such as equal opportunities monitoring); or
 - 2.3.4 in exceptional circumstances we may process this data with your explicit consent.
- 2.4 The Company also holds and processes the personal data of Employees' next of kin, family or friends for the purposes of emergency contact details and expression of wishes on insurance.
- 2.5 Please note that a refusal by you to provide the Company with the relevant personal data required to carry out the purposes listed above will significantly hinder the Company's ability to provide you with your employment rights and benefits and/or to comply with a legal obligation.
- 3. Collection, Use and Accuracy**
- 3.1 The Company obtains personal data about you from a number of sources including the application form or curriculum vitae you submitted when you applied to join, from interview notes, from third parties, such as recruitment agencies, Disclosure Scotland and the Disclosure and Barring Service in the event you are required to undergo a criminal conviction check, and from any details you subsequently provide us. We will also keep records of, for example, your absence history, your regular performance reviews and any actions or decisions taken as a result of applying any of our policies (in accordance with the terms of the relevant policy).
- 3.2 Respectable employment practice and the efficient running of the business require the Company to hold certain personal details about you on file. These personal details may include special categories of personal data about you, such as information on your health, race or ethnic origin or sexual orientation.

- 3.3 Within the Company, only Employees members with a right to access your personal and sensitive personal data will be able to do so. The Company takes steps to ensure that access to your personal data is only given to those who need such access. In particular, this includes your line manager / supervisor having access to relevant Personal Data such as your home address, home/mobile telephone number, marital status record, emergency contact details and absence records, authorised members of our Occupational Health team and HR teams having access to relevant occupational health information such as management reports produced following employee health assessments.
- 3.4 The Company will use the information held about you for purposes connected to your employment. For the purposes set out in paragraphs 1.2 and 2.3 the Company may transfer personal data to third parties. These are: insurers; legal advisors; medical advisors including occupational health service providers and consultants; professional advisors; Pension Schemes; Payroll suppliers; and Tax Authorities.
- 3.5 The Company may also transfer your personal data to its customers and their auditors to assist them in understanding the costs of contracts. Where possible, this personal data will be anonymised.
- 3.6 Personal data of a particular Employee may, at the request of that Employee, be shared with other third parties. They must first discuss this request with the relevant Data Protection Officer.
- 3.7 In line with the policy, the Company will make every effort to ensure that the information held about each Employee is accurate and, where necessary, kept up to date. It is your responsibility to ensure that your information contained in the HR database is accurate and kept up to date. In the absence of evidence to the contrary the Company shall assume that the information provided by you is accurate. If there is any reasonable doubt as to the accuracy of the data, the Company shall contact you to confirm the information. Should you inform us, or the Company otherwise becomes aware, of any inaccuracies in the information, the inaccuracies shall be rectified promptly.
- 3.8 An Employee must not pass any personal data relating to a colleague to any other person unless specifically authorised to do so by that person or by the relevant Data Protection Officer. If another person who is not a Data Protection Officer requests information about another person you are not authorised to disclose any such information and such request should be referred promptly to the Data Protection Officer.
- 3.9 Personal data may be shared between:
- 3.9.1 the parties listed in paragraph 3.3 and 3.4 above; and / or
- 3.9.2 the relevant entities within the Company's group, which may involve the sharing of your personal data outside of the EEA.
- 3.10 The Company is able to share your personal data as set out above as it has:
- 3.10.1 an agreement in place between the Company and third party suppliers of the Company in relation to where personal data is to be, on terms which protect such data and allow it to be shared outside of the EEA with such parties; and
- 3.10.2 a data sharing agreement in place between the Company's relevant group companies which protects the data. To request a copy of the relevant agreement, please contact the relevant Data Protection Officer.
- 4. Monitoring and Security**
- 4.1 The Company may monitor electronic communications by Employees and use of websites for the purpose of ensuring that the Company's IT systems are being used in accordance with the data protection policy and information security policy. Further details of the policy in relation to monitoring email and internet use can be found in the acceptable use policy which is available on the Company intranet.

5. Retention

- 5.1 The Company keeps Employees' personal employment files in soft/online format and hard copy.
- 5.2 A copy of our retention policy can be found on the intranet.

6. Data Portability

- 6.1 You are entitled to receive the personal data concerning you, which you have provided to the data controller, in a structured, commonly used and machine-readable format.
- 6.2 You have the right to transmit the personal data to another data controller, without hindrance where the processing is based on consent or the processing is carried out by automated means.
- 6.3 We do not consider that you will have a specific right to data portability in the context of your employment or engagement as:
 - 6.3.1 processing will not be carried out on the basis of consent; and
 - 6.3.2 no automated processing is carried out in respect of Employees

7. YOUR RIGHTS – EMPLOYEE QUESTION AND ANSWER

- 7.1 To exercise your rights as per this policy, you should apply in writing to the relevant Data Protection Officer.

8. Access your Personal Data

- 8.1 What happens next?

If you have any questions about data protection or your personal data, you should email dataprotection@balfourbeatty.com.

Your request will be dealt with promptly and the information to which you are entitled will be provided to you no later than one month (except in extenuating circumstances) from when we receive your request, subject to the requirements and exemptions of data protection laws. If such extenuating circumstances mean we are unable to comply with your request within one month, we will tell you as soon as possible about this delay.

- 8.2 Examples of exceptions, where the Company (by law) does not provide access to data include:
 - 8.2.1 References written by the Company;
 - 8.2.2 Any data from which a third party can be identified, unless it is possible to remove the identifying elements (e.g. by way of redaction);
 - 8.2.3 Any data held for the purposes of management forecasting or planning if access to the same is likely to prejudice the conduct of the Company's business;
 - 8.2.4 Any data prejudicing ongoing negotiations with the employee
 - 8.2.5 Any data protected by legal professional privilege; and/or
 - 8.2.6 Any data regarding an employee's health which an appropriate health professional considers likely to cause serious harm to the employee's physical or mental health or of any other person.

9. Request Your Data is Rectified

- 9.1 When?

You should request that your data is rectified either where the personal data is inaccurate or to request we complete any incomplete information (e.g. by way of supplementary statement).

9.2 What happens next?

Your request will be dealt with promptly and without undue delay.

10. **Request Your Data is Deleted**

10.1 When?

You have a right to request the Company deletes information held about you in certain circumstances (e.g. where we no longer have the right to process the information). If you wish the Company to delete some (or all) of your personal data, you should apply in writing to the relevant Data Protection Officer.

10.2 What happens next?

Your request will be dealt with promptly and without undue delay, subject to the requirements and exemptions of the data protection laws. In some circumstances the Company will be unable to comply with your request, for example if the Company has legal duties or obligations to continue processing the data. It is unlikely the Company will be able to erase certain information whilst you remain an employee, as it will be necessary for the purposes of your continuing employment and to meet our obligations in relation to tax and other regulatory duties. This will be addressed on a case by case basis following a request for erasure.

11. **Restrict or Object to Processing**

11.1 When can I obtain from the Company a restriction of processing?

Where:

- (a) you contest the accuracy of the personal data (and so processing will be restricted for a period of time which will enable the Company to verify the accuracy of the personal data);
- (b) the processing is unlawful and you oppose the erasure of personal data and request restriction instead;
- (c) the Company no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of a legal claim;
- (d) you have objected to the processing on the basis of the Company's legitimate interests pending the verification of whether such legitimate grounds override yours.

11.2 What does restriction mean?

With the exception of storage, the Company will only be able to process the personal data with your consent or for the establishment, exercise or defence of legal claims or for the protection of another natural or legal person or for reasons of important public interest.

12. **When can I object to the Company processing my personal data?**

12.1 You can object to the Company processing your personal data where the Company is processing your personal data on the basis of its legitimate interests, including profiling. To the extent the Company cannot demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms the Company will no longer process your personal data for these purposes.

13. Complain

13.1 To the Company

If you have a complaint or concern around the use of your personal data in the context of your employment or engagement with the Company, please discuss this with the relevant Data Protection Officer in the first instance.

13.2 To the Supervisory Authority

In the event you are dissatisfied with the response of the Data Protection Officer, you have the right to complain to the Supervisory Authority.

14. Reporting

15. To the Company

All Employees must report any actual or suspected breaches of data protection law to a Data Protection Officer as soon as possible on becoming aware of such incidents by emailing dataincident@balfourbeatty.com.

16. Additional Contact Information

16.1 If you have any questions or concerns around how your personal data is being collected, used or stored, please discuss this with the Data Protection officer for your business unit in the first instance or email dataprotection@balfourbeatty.com with your query.

16.2 Data Protection Officer Details

Name	Business Unit	Contact Details
Chris Johnson	Chief Information Officer & Serious Information Risk Owner	chris.johnson@balfourbeatty.com
Matthew Kay	Group Data Protection Officer	matthew.kay@balfourbeatty.com
Nick Lee	Employee Services	nick.lee@balfourbeatty.com
Rachel Taylor	Enabling Functions	rachel.taylor@balfourbeatty.com
Maxine Wheldon	Major Projects	Maxine.wheldon@balfourbeatty.com
Jenni Morris	UKCS	Jennifer.morris@balfourbeatty.com
Rachel Byrne	Rail, Power T&D	rachel.byrne@balfourbeatty.com
Sharon Thomson	Gas & Water	Sharon.thomson@balfourbeatty.com
Christina Brown	Highways, Plant & Fleet, Investments	Christina.brown@balfourbeatty.com