Privacy notice for employees

This notice explains how we obtain, use and erase personal data (information) about our employees, workers and applicants. The notice is also intended to ensure that employees ('you') understand and comply with the rules governing the collection, use and deletion of personal information to which you may have access to in the course of your work. Please ensure that you read this notice and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

1. Who collects the information?

The Hills Group Limited (the company) is a 'data controller' for the purposes of the General Data Protection Regulations (GDPR) and gathers and uses certain information about you.

This information is also used by other Group companies including: Hills UK Ltd, Hills Waste Solutions Ltd, Hills Municipal Collections Ltd, Hills Quarry Products Ltd and Hills Homes Developments Ltd, and so in this notice, reference to 'the company', 'we' or 'us' mean the company and our Group companies.

2. Data protection principles

We will comply with the data protection principles when gathering and using your personal information, as set out in our Data Protection Policy. This policy can be obtained on eTouch or requested from your line manager, the HR department or the Company Secretary's office.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any material changes to information we collect or the purposes for which we collect and process it.

3. How your information will be used

3.1 As your employer, the company needs to keep and process information about you. This information enables us to run the business and manage our relationship with you effectively, lawfully and appropriately. We may gather and process information about you during the recruitment process, during your employment and after your employment ends.

We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will only use your personal information when the law allows us to.

We will typically collect and use this information for the following purposes:

- For the performance of a contract with you, or to take steps to enter into a contract
- For compliance with a legal obligation (eg our obligations to you as your employer under employment protection and health and safety legislation, and under statutory codes of practice, such as those issued by ACAS)
- For the purpose of our legitimate interests (eg to comply with legal reporting obligations, to protect our business assets, to prevent fraud) or those of a third party (such as a benefits provider), but only if these legitimate interests are not overridden by your interests, rights or freedoms
- To protect our legal position in the event of legal proceedings.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests)
- Where it is needed in the public interest or for official purposes.

3.2 We may collect the following information from you during your employment:

- Your name, contact details (ie address, home and mobile phone numbers, email address) and emergency contacts (ie name, relationship and home and mobile phone numbers)
- Information collected during the recruitment process that we retain during your employment

- Employment contract information
- Details of salary and benefits, bank/building society, National Insurance and tax information, your age
- Details of your spouse/partner and any dependants
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information
- A copy of your driving licence (if required for your employment with the company)
- Details of your pension arrangements all information included in these and necessary to implement and administer them
- Occupational health records
- Information on your sickness and absence records (including sensitive personal information regarding your physical and/or mental health)
- Information needed for equal opportunities monitoring
- Criminal records monitoring
- Your trade union membership
- Information on grievances raised by you or involving you
- Information on conduct and/or other disciplinary issues involving you
- Details of your appraisals and performance reviews
- Details of your qualifications and training records
- Details of your performance management/improvement plans (if any)
- Details of your attendance and hours worked
- Accident reports
- Information in applications you make for other positions within our organisation
- Information about your use of our IT, communication and other systems, and other monitoring information
- Details of your use of business-related social media such as LinkedIn and company websites
- Public social media (only in very limited circumstances in relation to complaints or inappropriate use)
- Details in references about you that we give to others
- Correspondence with or about you, eg letters to you about a pay rise or, at your request, a letter to your mortgage company.

3.3 You may be referred to in documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company. In pursuing the company's legitimate business interest, documents and reports may also be produced to be issued to third parties that include information about you, eg details of your qualifications or core competencies in a tender document for new business.

3.4 Where necessary, we may keep information relating to your health, which could include reasons for absence and GP reports and fit notes that you provide us. This information will be used in order to comply with our health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay or life assurance policies. Where you are in agreement and it is necessary to provide this information to a third-party medical advisor we will seek your consent before transferring this information.

3.5 We will only collect sensitive information relating to your racial or ethnic origin, religion, protected characteristic, and sexual orientation with your consent, and where it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing such as it is in the public interest to do so. Where this information has been provided it may be anonymised, aggregated and used to provide statistical monitoring and reporting of diversity and equality within the company's employee base. Other personal data may be anonymised, aggregated and used to provide statistical monitoring and reporting this includes training records, causes of absenteeism and accident reports.

3.6 In addition, we monitor computer and telephone/mobile telephone use, posts on our company websites and social media platforms. We will also investigate, when brought to our attention, if an employee's social media use is in breach of company policy, as detailed in our Acceptable Use and Code of Conduct Policy, available in the employee handbook and available on eTouch or on request from your line manager, HR department or Company Secretary's office.

This information will enable us to monitor and manage employee access to our systems and facilities, to protect our networks and the personal data of employees and customers / clients against unauthorised access or data leakage, and to ensure our business policies and contractual restrictions are adhered to.

3.7 Where installed we also keep records of your hours of attendance at work by way of the building or places of work security access control or attendance systems. This information is used to confirm attendance, employee presence in the event of an evacuation and for building security purposes.

3.8 The company operates CCTV monitoring systems at a number of its sites and 4 way camera systems are installed on LGV vehicles. Depending on the system, video data captured is over written up to 30 days following its recording.

CCTV monitoring systems are used for maintaining site and building security (including access and egress) and asset protection. Vehicle 4 way systems are primarily installed to assist the driver to the presence of an individual or obstacle and are also used in accident investigation.

Video data is only reviewed and retained beyond 30 days for the purposes of investigating:

- A security incident; or
- An accident or incident where health and safety risk, personal injury, property damage or theft is either alleged or has actually occurred and it is in the company's overriding legitimate interest to investigate.

Video data retained for these purposes may be used in disciplinary procedures and disclosed to enforcement agencies and insurance companies. With an employee's consent video showing their involvement in a near miss or incident may be used for the purposes of health and safety training.

3.9 All LGV vehicles are fitted with telematic systems to monitor speed and location of the vehicle. The data collected is reviewed by relevant transport managers to monitor driving standards of drivers and may be used in accident reports, motor insurance claims and investigations into allegations of speeding and breaches of road weight restrictions by drivers. Telematic data may be used in company disciplinary procedures and disclosed to enforcement agencies and insurance companies.

Some vehicles have collection/delivery routing systems installed on the dashboard that record the activity of the vehicle and location. Data from this system may be reviewed by transport managers in order to verify the performance of vehicle and its crew and may be used in company disciplinary procedures.

3.10 If you are a professional driver required to drive a vehicle for your job role you will be asked to provide a copy of your driving licence and also complete a D906 form to consent the company to have access to your driving records held by the DVLA via a secure online portal.

If you are a professional driver you will be required to supply a copy of your Driver Certificate of Professional Competence to be held with your employment records. Further details on employee driver record checking can be found in the handbook issued to all van and LGV drivers.

4. Accuracy of information

Much of the information we hold will have been provided by you and you are responsible for ensuring that the information you provide us is accurate and up to date. It is therefore important that you notify your manager or HR department promptly of any changes to the information you have provided to us. Some of the information we hold about you may come from other internal sources such as your manager, or in some cases, external sources such as referees.

5. How we may share the information

5.1 We will only disclose information about you to third parties:

- Where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to our external payroll provider, pension or life assurance scheme
- If we are legally obliged to do so (eg tax authorities and potential purchasers under the Transfer of Undertakings legislation), or
- The business has an overriding legitimate business reason (eg with legal advisers or regulators in the event of an internal or legal process).

'Third parties' include third-party service providers (including contractors and designated agents). The activities carried out by third parties include but are not limited to payroll, pension administration, benefits provision and administration, IT services.

Where we transfer data to a third party we will do so in a secure manner in accordance with our Data Protection Policy and ensure that it is processed in accordance with the GDPR.

5.2 All our third-party providers are required to take appropriate security measures to protect your personal information in line with our policies. Unless otherwise notified to you, we do not allow our third parties to use our personal data for their own purposes. We only permit them to process your personal data for specified purposes in accordance with our instructions.

5.3 We may share your personal information with other third parties, for example in context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

5.4 If you communicate with us through a third-party system such as a social media platform, personal email or personal IT system please remember that we do not control these third-party websites or systems and are not responsible for their privacy statements.

We encourage you to read the privacy notice of every website or forum that you visit or use to communicate with us.

5.5 We may also need to share your personal information with a regulator or to otherwise comply with the law.

5.6 We may transfer information about you to other Group companies for purposes connected with your employment or the management of the company's business and there is a legitimate business reason (eg for independence in the operation of our disciplinary and grievance procedure, site management and business continuity).

5.7 In limited and necessary circumstances, your information may be transferred outside of the European Economic Area. If this is required we will ensure adequate safeguards are in place to ensure the security of your data in accordance with the GDPR.

6. Retention of data

Your personal employment data will be stored for a period of not more than four years from the date your employment ceases to the end of that financial year (30 April) plus three years. For example: if your employment ceased on the 23 January 2019 your records would be held until 1 May 2022. This is in order for us to meet our legitimate business needs and will be disposed of in a secure manner after this time unless:

- We are obliged to hold it for a longer period in accordance with statutory purposes, for example mandatory occupational health records
- To fulfil a contractual requirement to you (eg in order to make pension payments)
- The business has an overriding legitimate business reason to continue to hold the information.

7. Change of purpose

7.1 We will only use your personal information for the purposes for which we have collected it, unless we consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

7.2 Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

8. Documentation and records

8.1 We will keep records of processing activities which are high risk, ie which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information.

8.2 We will conduct regular reviews of personal information we process and update our documentation accordingly, eg information audits, distributing questionnaires, reviewing policies, procedures and contracts.

9. Further detail

A schedule that summarises the information we collect and hold, how and why we do so, how we use it and with whom it may be shared is published on eTouch or can be requested from your line manager, the HR department or the Company Secretary's office.

10. Your rights and obligations

10.1 Under the GDPR you have a number of rights with regard to your personal data. You have the right to:

- Be informed about how, why and on what basis information is being processed
- Obtain confirmation that your information is being processed and to obtain access to it by making a subject access request
- Request from us access to and rectification if it is inaccurate or incomplete
- Request erasure of your personal data if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (also known as 'the right to be forgotten')
- Restrict process where the accuracy of the information is contested, or the processing is unlawful, but you do not want the data to be erased, or we no longer need the personal information, but require the data to establish, exercise or defend a legal claim
- Restrict the processing of personal information temporarily where you do not think it is accurate or where you have objected to the processing and we are considering whether our legitimate interests override your interests.

10.2 If you wish to exercise any of the rights listed above, you should contact the Data Protection Officer (as detailed on page 6).

10.3 You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

10.4 If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

11. Right to withdraw consent

If you have provided consent for the collection, processing and transfer of your data for a specific purpose, you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.

To withdraw your consent, please contact the Data Protection Officer (as detailed below). If you withdraw your consent for the company to process certain types of data, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

12. Your Data Protection Officer

If you have any concerns as to how your data is processed you can contact:

Alex Henderson, Company Secretary who acts as the Data Protection Officer at:
alex.henderson@hills-group.co.uk
or you can write to:
The Company Secretary, Wiltshire House, County Park Business Centre, Shrivenham Road, Swindon, SN1 2NR.