GDPR PRIVACY NOTICE:
ALL BREEDON GROUP WORKERS

v7.0

September 2026

GDPR PRIVACY NOTICE FOR ALL BREEDON GROUP WORKERS

What is the purpose of this document?

Breedon Group plc and its subsidiaries, are committed to protecting the privacy and security of your personal information.

Breedon Group plc has the following wholly owned trading subsidiaries: Breedon Trading Limited, Breedon Cement Limited, Breedon Holdings Limited, Breedon Group Services Limited, Breedon Materials Limited, Breedon Surfacing Solutions Ireland Limited, Whitemountain Quarries Ltd, Alpha Resource Management Ltd, Breedon Cement Ireland Limited, Breedon Employee Services Ireland Limited, Breedon Brick Limited (together **Breedon** and each a **Breedon Company**).

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the EU General Data Protection Regulation (Regulation (EU) 2016/679) and the UK GDPR as defined in section 3(10) of the Data Protection Act 2018 (**GDPR**).

It applies to all Breedon workers, "worker" means all of Breedon's permanent and temporary employees, work experience candidates, agency workers, consultants, company officers, directors, job applicants, contractors and workers.

Each Breedon Company is a "data controller", which means a party who (either alone or jointly) determines the purposes for which and the manner in which any personal data is, or will be, processed. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former workers. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

Identity Data:

- Personal contact details such as name (surname and forenames), title, addresses, telephone numbers, and personal email addresses; date of birth; gender; nationality; marital status and dependants (including your potential beneficiary details in relation to life assurance, death in service or personal pension (if any)); next of kin and emergency contact information; copy of passport including photograph; copy of driving licence, insurance certificates, recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process; interview notes, internal notes, results of any written or online selection tests); photographs; automated voice recording from our telephone systems.

Financial Data:

- Bank account details, payroll records and tax status information; salary; annual leave; pension details and rates; benefits information; National Insurance number or Irish equivalent; tax code; cumulative taxable pay and tax; cumulative NIable pay and NI; breakdown of NI; payroll number; bank sort code and account number; bank account name; building society roll number; student loan information; court order information; share scheme or share save details; compensation history.

Worker Data:

- Start date; reason for leaving and date; annual leave; FTE and contract hours; full or part time; working pattern; location of employment or workplace; employment records (including job titles, work history, training records and professional memberships); performance information; disciplinary and grievance information; mobile phone records; information about your use of business equipment, technology and systems including our computers, telephones, mobile phones, software applications, social media, door entry systems, clocking in and out systems and/or time recording; vehicle registration numbers or mileage records;

CCTV footage and other information obtained through electronic means such as swipecard records, route mapping data; information about your use of our information and communications systems; information obtained from onboard CCTV or vehicle tracking systems.

We may also collect, store and use the following "special categories" of more sensitive personal information:

Special Category Data:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions; Trade union membership; Information about your health, including any medical condition, health and sickness records including breakdown of SSP, SMP and SPP; medical screening information; and/or Information about criminal convictions and offences.

Technical Data:

- Internet protocol (IP) address; your login data; browser type and version; time zone setting and location; browser plug-in types and versions; operating system and platform; and other technology on the devices you use to access this website.

Usage Date:

- Information about how you use the internet; username; passwords; and browser history, from any devices belonging to the Breedon Group.

How is your personal information collected?

We collect personal information about workers through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider.

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

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

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

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest.

Situations in which we will use your personal information

We need all the categories of information in the list above (see "The kind of information we hold about you") primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will normally process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK or Ireland and obtaining references.
- Paying you correctly and determining overtime and, if you are an employee, deducting tax and National Insurance contributions (or equivalent under Irish tax laws) and keeping appropriate records.
- Providing the following benefits to you, such as but not restricted to: company vehicles, private healthcare, death in service, mobile phone.
- Liaising with your pension provider.
- Ensuring you are appropriately qualified and trained for current or potential roles.
- Administering, managing and enforcing the contract we have entered into with you.
- Providing access to the Breedon Sharesave Scheme or other share scheme and administering this or appointing third parties to administer this on our behalf.
- Business management and planning, including accounting and auditing, business efficiencies and improvements.

- Conducting performance reviews, managing performance and determining performance requirements.

- Making decisions about salary reviews and compensation.

- Assessing qualifications for a particular job or task, including decisions about promotions and career progression.

- Gathering evidence for possible grievance conduct or disciplinary hearings or breaches of contractual obligations related to you or otherwise involving you.

- Making decisions about your continued employment or engagement.

- Making arrangements for the termination of our working relationship.

- Education, training and development requirements.

- Dealing with legal disputes involving you, or other workers, including but not limited to verification of information provided and accidents at work.

- Conducting risk assessments, establishing safety measures to mitigate identified risks; providing a safe working environment and keeping required records.

- Ascertaining your fitness to work.

- Managing sickness absence, statutory and non statutory holiday and other leave.

- Complying with health and safety obligations.

- To prevent fraud.

- To monitor your use of our information and communication systems and social media presence to ensure compliance with our IT policies and expected standards.

- Recording communications with customers for quality control and training purposes.

- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution; preventing excessive personal use.

- To conduct data analytics studies to review and better understand employee retention and attrition rates.

- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

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).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably 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.

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.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations and in line with our Data Privacy and Protection Policy.

3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our Data Privacy and Protection Policy.

4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations in relation to special categories of data

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

- We will use information relating to leaves of absence, which may include sickness absence or family related leave in gathering evidence for possible grievance or disciplinary hearings or making decisions about your continuing employment or engagement.

- We may collect limited information from you which can be in the form of an "expression of wishes" which sets out how and to whom you would like us to distribute the proceeds of any company benefits we administer (**Beneficiary**). This could include life assurance or death in service benefit. We obtain the details (name and relationship to you) of the Beneficiary from you under an obligation of confidence and will only be processed, when we need to administer the relevant benefits. We are prevented from notifying a Beneficiary of the details of the personal data we hold about them as the information was obtained under an obligation of confidence. You may provide personal data of a Beneficiary directly to a third party benefits provider as part of your employment which will be processed in line with that third party's privacy policy and notices.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Data Privacy and Protection Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

Where appropriate, we will collect information about criminal convictions as part of the recruitment or appointment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- Making a decision about your recruitment or appointment.
- Making decisions about your confirmed employment or engagement
- Making arrangements for the termination of our working relationship.

We are allowed to use your personal information in this way to carry out our legal obligations and in our legitimate interests to determine any impact of those criminal convictions within a particular role.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, making payments to you, pension administration, benefits provision and administration, IT services, Sharesave or share scheme provision and administration, mileage logs, vehicle tracking, CCTV monitoring, phone recordings. This includes but is not limited to the following third-party service providers who may process personal information about you for the following purposes:

- Midland HR iTrent (payroll); Sage (accounts & payroll packages); Pams (HR software); CORVID PayGate and Experian (Bacs payment software); Concur Solutions (expenses software); Link Asset Services and Orient Capital (shareholder registry); Aon Hewitt (management consultancy); Aviva (pension provider, private medical insurance, life assurance and digital GP); Willis Towers Watson (benefits broker and insurance broker); AXA (motor insurance); HDI Global (to deal with employer's liability claims); Peoples Pension (pension provider); Legal and General (life assurance provider); Yorkshire Building Society (Sharesave scheme); TomTom (route tracker); Barclays (our bankers); Danske (banking); Zenith (company cars); HMRC (to deal with taxation); Inform Direct (statutory records); SAP (computer system); JDE (computer system); Quiet Storm Ltd (communications distributor); SunSign Communications, MED Ltd, Quiet Storm Ltd and Radley Yeldar (photographs from publications); Investis Limited (website host via the systems of Bladonmore (Europe) Ltd); Evolve, Kevin Bradly Ltd (courier); Parcelforce (courier); Postal Sort (postal services); Fisher German (tenant agency); Occupational Health practitioner; Simply Health, Westfield Health (health insurance providers); Kerr Henderson (life assurance broker); GMB, Unite Union (Union fees); Welfare Hope (Hope social club contribution); Curie Care, Charitable Giving,

Barnado's (charitable donations); Court Orders (payments by employees re judgments); Student Loans (payments by employees for historical loans); professional trustees; the Company's brokers; Insight (despatch software); SHE (HSE software); ZAP (Business Intelligence Tool); Therefore (Canon Document Management); and/or Advance Systems (Time & Attendance System).

We also share data with our legal and other professional advisers appointed from time to time to obtain professional advice about matters relating to you or in the course of dealing with disputes with you and other workers or in compliance with our legal obligations.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance where we need to perform our contract with you, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data, for business improvements, to protect health and safety, for learning and development.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

We may also share your data with potential new service providers or other corporate transactions.

We will share your data with customers, potential customers, shareholder and interested parties for inclusion in corporate reports for use in business communications and/or security clearance to work on customer's premises.

Transferring information outside the EEA

We will transfer the personal information we collect about you to countries outside the EEA in order to perform our contract with you. We will only do this if there is an adequacy decision by the European Commission in respect of that country or we will ensure that the recipient of the information enters into a contract with us confirming that your personal information does receive an adequate level of protection as it were in the EEA. If you require further information about these protective measures, you can request it from the Compliance Team.

Data security

We have put in place measures to protect the security of your information.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of data retention periods for different aspects of your personal information are available in our Data Retention Schedule which is available from the intranet (if relevant) or the Compliance Team. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our Data Retention Schedule or any applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

- **Raise a complaint** about the processing of personal information.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact a member of the Compliance Team in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact a member of the Compliance Team. Once we have received notification that you have withdrawn your consent, 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. Please note we are not necessarily obliged to accept your withdrawal request. There may be other legal reasons why we can refuse.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Make a Complaint

You may make a complaint to the local data commissioner's office in which the Company operates if you are dissatisfied as to how your personal data is being processed. In the first instance you can also make a complaint to the Company by emailing legal.compliance@breedongroup.com