

TILlicOUNTRY QUARRIES

Data Protection Policy

1 INTERPRETATION

- 1.1 In this policy a reference to “we” or “us” is a reference to Tillicoultry Quarries Limited. References to “you” are references to the employee or worker covered by this policy.
- 1.2 “Third parties” includes third party service providers (including contractors and designated agents).
- 1.3 “DCM” means Tillicoultry Quarries Limited’s Data Compliance Manager, who can be contacted at Northfield Quarry.

2 INTRODUCTION

- 2.1 As a “Data Controller” we are responsible for deciding how we hold and use personal data (sometimes referenced as personal information) about you. We are committed to protecting the privacy and security of personal data. This policy is issued so that you are aware of our approach to the management of personal data.
- 2.2 This policy describes how we collect and use personal data in accordance with the General Data Protection Regulation (“GDPR”). This policy also sets out the responsibilities of individuals in respect of any personal data they may handle and use in the course of working for or providing services to us.
- 2.3 We have, in advance of issuing this policy, reviewed the technical and other measures adopted by us to ensure compliance with data privacy principles.
- 2.4 It is important that you read and act in accordance with this policy. It sets out what we expect from you and compliance is mandatory. Any breach of this policy may result in the termination of any contract and/or disciplinary action.

3 RESPONSIBILITY

The DCM is ultimately responsible for ensuring compliance with this policy and all supervisors and managers are required to ensure that its standards are maintained. Equally, everyone working for us must comply with its terms. If you have any questions about this policy or how we handle personal data, please contact the DCM. You also 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.

4 PRIVACY NOTICE

This policy amounts to a privacy notice for the purposes of the GDPR and contains all of the information which we are required to provide to you under data protection legislation.

5 SCOPE

This policy applies to all employees and workers (including former employees and workers) who are employed or engaged by us. This policy does not form part of any contract of employment or other contract to provide services.

6 ACCOUNTABILITY

We will make sure we have in place appropriate measures to ensure compliance with the GDPR and this policy, and where appropriate we will carry out and document risk assessments.

7 DATA SECURITY

7.1 We have put in place measures to protect the security of your personal information. Details of these measures are available and can be requested from the DCM. These 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 and third parties who have a business need to know.

7.2 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.

8 RECORD KEEPING

Responsibility for record keeping relative to our data processing activities is the responsibility of the DCM.

9 CORE PRINCIPLES

The law says that the personal information we hold about you must be:

- 9.1 Used lawfully, fairly and in a transparent way.
- 9.2 Collected only for legitimate purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- 9.3 Relevant to the purposes we have told you about and limited only to those purposes.
- 9.4 Accurate and kept up to date.
- 9.5 Kept only for as long as is necessary for the purposes we have told you about.
- 9.6 Kept securely.

10 PERSONAL DATA

- 10.1 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).
- 10.2 There are “special categories” of more sensitive personal data which require a higher level of protection.
- 10.3 The categories of data that we will collect, store and use will depend on your status. It will also depend on the role held by you. The following lists the data we will hold, store and collect:
 - 10.3.1 Personal contact details such as name, date of birth, gender, marital status and dependents, addresses, telephone numbers, and personal email addresses;
 - 10.3.2 Next of kin and emergency contact information;
 - 10.3.3 Payroll information (including National Insurance numbers, bank account details, payroll records and tax status information);
 - 10.3.4 Salary, annual leave, absence dates, pension and benefits information;
 - 10.3.5 Identification documents (including passports and driving licences);

- 10.3.6 Recruitment information (including copies of right to work documentation, references and other information included in a CV, application form or cover letter or as part of the application process);
 - 10.3.7 Employment records (including job titles, work history and location, working hours, training records and professional memberships);
 - 10.3.8 Performance, disciplinary and grievance information;
 - 10.3.9 Documentation and professional certificates, approvals or licences where applicable;
 - 10.3.10 CCTV footage and other information obtained through electronic means such as swipecard records;
 - 10.3.11 Information about your use of our information and communications systems; and
 - 10.3.12 Photographs.
- 10.4 We may also collect, store and use the following “special categories” of more sensitive personal information:
- 10.4.1 Information about your health, including any medical condition, health and sickness records.

11 HOW IS YOUR PERSONAL INFORMATION COLLECTED?

- 11.1 We collect personal information about employees and workers through the application, recruitment and induction process, either directly from individuals or sometimes from an employment agency or background check provider. We may sometimes collect additional information which is publicly available or further information from third parties including former employers, credit reference agencies or other background check agencies. Data may also be received from our occupational health providers.
- 11.2 We will collect additional personal information in the course of job-related activities throughout the period you are working for us.

12 HOW WE WILL USE INFORMATION ABOUT YOU?

- 12.1 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:
 - 12.1.1 Where we need to perform the contract we have entered into with you;

- 12.1.2 Where we need to comply with a legal obligation; or
 - 12.1.3 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.
- 12.2 In particular, the situations in which we may process your personal information are as follows:
- 12.2.1 Determining the terms on which you work for us including, where required, making arrangements for the termination of our working relationship;
 - 12.2.2 Checking you are legally entitled to work in the UK;
 - 12.2.3 Administering the contract we have entered into with you including identifying education, training and development requirements;
 - 12.2.4 Paying you and, if you are an employee, deducting tax and National Insurance contributions;
 - 12.2.5 Providing benefits to you (including liaising with your pension provider and managing any stock or share option schemes which you may be a part of);
 - 12.2.6 Business management and planning, including accounting and auditing;
 - 12.2.7 To carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
 - 12.2.8 Dealing with legal disputes involving you, or other employees, workers, contractors or third parties, including accidents at work and complying with health and safety obligations;
 - 12.2.9 Managing your sickness absence, ascertaining your fitness to work and communicating with our providers of private medical cover or other insurance cover;
 - 12.2.10 Monitoring your use of our information and communication systems;
 - 12.2.11 Monitoring compliance by you, us and others with our policies and our contractual obligations;
 - 12.2.12 Prevention and detection of fraud or other criminal offences;
 - 12.2.13 To provide a reference upon request from another employer;
 - 12.2.14 to answer questions from insurers or mortgage providers in respect of any policies which relate to you; and

12.2.15 Dealing with necessary due diligence in connection with any business transfer.

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

13 **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). Any failure may result in a contract with you being terminated or the taking of disciplinary action.

14 **CHANGE OF PURPOSE**

14.1 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.

14.2 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.

15 **HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION**

15.1 “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:

15.1.1 In limited circumstances, with your explicit written consent;

15.1.2 Where we need to carry out our legal obligations;

15.1.3 Where it is needed in the public interest, such as in relation to our occupational pension scheme;

15.1.4 To determine whether we need to make reasonable adjustments to your workplace or role because of a disability;

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

15.2 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.

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

15.3.1 We will use information relating to absence which may include sickness absence or family related leave to comply with employment and other laws;

15.3.2 We will use information relative to health where appropriate in the context of our provision of private medical cover; and

15.3.3 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.

16 DATA SHARING

16.1 We may have to share your data with third parties.

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

17 WHY MIGHT WE SHARE YOUR PERSONAL INFORMATION WITH THIRD PARTIES?

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

18 WHICH THIRD PARTY SERVICE PROVIDERS WILL PROCESS YOUR PERSONAL INFORMATION

At the date of this policy, the following activities are carried out by third party service providers: pension administration; benefits provision and administration; occupational health and the provision of private medical care.

19 HOW SECURE IS YOUR INFORMATION WITH THIRD PARTIES?

All our third-parties 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.

20 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.

21 TRANSFERRING INFORMATION OUTSIDE THE EUROPEAN ECONOMIC AREA (“EEA”)

21.1 We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

22 DATA BREACHES

22.1 As a Data Controller, we have certain legal obligations under the GDPR to notify the ICO in the event of the loss or unauthorised access, disclosure or acquisition of the personal information we hold (“**Data Breach**”).

22.2 If you know or suspect that a Data Breach has occurred, do not attempt to investigate the matter yourself. Please contact the DCM immediately and follow their instructions. You should preserve all evidence relating to the potential Data Breach.

23 HOW LONG WILL WE USE YOUR INFORMATION FOR?

23.1 We will only retain your personal information for as long as is necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.

23.2 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.

23.3 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 at the appropriate time securely destroy your personal information in accordance with the terms of the foregoing paragraph.

24 YOUR RIGHTS IN CONNECTION WITH PERSONAL INFORMATION

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

24.1.1 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;

24.1.2 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;

24.1.3 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);

24.1.4 Object to the processing of your personal information where we are relying on a legitimate interest (or a legitimate interest of a third party) and there is something about your particular situation which makes you want to object to processing on this ground;

24.1.5 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; and

24.1.6 Request the transfer of your personal information to another party.

24.2 If you want to access, verify, correct or request erasure of your personal information, object to or restrict the processing of your personal information, or request that we transfer a copy of your personal information to another party, please contact the DCM in writing.

24.3 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.

24.4 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.

25 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 the DCM. 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.

26 YOUR RESPONSIBILITIES

26.1 You are responsible for helping the organisation keep your personal data up to date. You should let us know if personal information you have provided to the organisation changes, for example if you move house or change bank details.

26.2 You may have access to the personal information of other individuals, customers and clients in the course of your working relationship with us. Where this is the case, we rely on you to help us meet our data protection obligations to staff, customers and clients.

26.3 In particular, if you have access to the personal information of others, you are required:

26.3.1 To only access personal information that you have authority to access and only for authorised purposes;

26.3.2 To only disclose personal information to individuals (whether inside or outside the organisation) who have appropriate authorisation;

26.3.3 To keep such personal information secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

26.3.4 Not to make unnecessary copies of personal data and should keep and dispose of any copies securely;

26.3.5 Not to remove personal information, or any devices which contain or which can be used to access personal information, from our premises without adopting appropriate security measures (such as encryption or password protection) to secure the information and the device; and

26.3.6 Not to store personal information on local drives or on personal devices that are used for work purposes.

26.4 In addition you must:

- 26.4.1 Ask the DCM or your line manager if you are unsure about this policy or any aspects of data management;
- 26.4.2 Advise the DCM if you become aware of any act or omission that has or risks compromising the security, confidentiality or integrity of personal data;
- 26.4.3 Consult the DCM if you are involved or may be involved in any major change of process or system that involves the processing of personal data as this may require that a data protection impact assessment is carried out;
- 26.4.4 Consult the DCM if you make use of automated processing or decision taking unless that has been previously approved;
- 26.4.5 Immediately forward on any data subject access requests which you may receive to the DCM who will coordinate a response;
- 26.4.6 Complete all mandatory data protection training; and
- 26.4.7 Make sure you do not hold personal data otherwise than in accordance with this policy and all applicable rules and regulations we may lay down from time to time and comply with all instructions to delete data given to you.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the company's disciplinary procedure.

27 **CHANGES TO THIS POLICY**

- 27.1 We reserve the right to update this policy at any time, and we will provide you with a new policy 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.
- 27.2 If you have any questions about this policy, please contact the DCM.