

This document sets out Mackenzie Construction's policy on the protection of information relating to Employees. It covers personal data relating to Employees who can be identified from the data, and which is either processed automatically, e.g. through a computer, or held on video, or else forms part of a filing system e.g. personnel records.

The Company will ensure that data is always processed in accordance with the provisions of the Data Protection Act 1998 & GDPR 2018.

In processing data, the following principles will be adhered to:

- Personal data will be processed fairly and lawfully. Normally, the Company will seek to obtain the consent of the Employee to the processing of personal data. In relation to the processing of sensitive personal data (which is personal data relating to race/ethnic origins, political, religious or other similar beliefs, sexual life, medical condition, commission of any offence, criminal proceedings or sentences, or trade union membership), explicit consent to any processing will normally be obtained.
- Personal data will be obtained for one or more specified and lawful purposes and will not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data will be adequate, relevant and not excessive.
- Personal data will be accurate and, where appropriate, kept up to date.
- Personal data will not be retained for longer than is necessary.
- Personal data will be processed in accordance with the rights of data subjects as defined by the 1998 Act.
- Appropriate measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data will not be transferred to countries outside the European Economic Area unless there are adequate measures in place to protect data subjects (Employees).

Access to Data

Employees have the right to request that the Company specify whether personal data of which he or she is the subject is being processed by the Company and to be given a description of the data, the purposes for which it is being processed and to whom it may be disclosed.

Employees have the right to obtain a copy of any personal data held. To exercise this right a written request should be made to our HR Manager specifying the information sought. A charge of £10 will be made for the information and, in accordance with the 1998 Act, shall be provided within the 40-day period following the date on which the Company is in receipt of both the written request and the £10 charge. Note that information requested which contains details relating to another individual will not normally be released (except in amended form) without that individual's consent. In addition, the Company will not normally release any information relating to references given by the Company on behalf of the Employee, management planning, information relating to negotiations with an Employee, e.g. over pay or any other information it is entitled to withhold under the 1998 & GDPR 2018 Act.

Processing of Data

The Company will conduct regular reviews of the information held by it to ensure the relevancy of the information it holds. Data will normally only be held for a limited period of time. Where an Employee leaves the Company, personal data will be kept only for such a period as may be necessary to protect the interests of the Company and the Employee.

Employees are under a duty to inform the Company of any changes to their current circumstances. Where an Employee has concerns regarding the accuracy of personal data held by the Company, the Employee should contact the HR Department to request an amendment to the data.

Security of Data

The Company will take appropriate measures to prevent unauthorised access to personal data and in particular any sensitive personal data held.

DATA PROTECTION & PRIVACY NOTICE POLICY

Access to personal data by managers and other Employees of the Company will be restricted only to those individuals who have legitimate business reasons for requiring the information.

Not only could such an event cause adverse publicity for the Company but, if the Employee is the person responsible for the infringement, the Employee could be the subject of a personal criminal prosecution and liable to a fine. It is important to keep the penalties in perspective, however. If the Employee follows the advice given below and takes sensible and reasonable precautions to protect information in the Employee's case there should be few, if any, problems.

- Observe to the letter any instruction or guidelines issued by the Company in relation to data protection and your work.
- Observe the data protection principles set out in the 1998 Act at all times.
- Take confidentiality and security seriously whether the Employee considers the information to be sensitive or not. In particular: -
 - do not disclose your password;
 - change your password regularly;
 - do not gossip about Company data;
 - do not leave Company data in the street, on the train, or on the bus etc.;
 - do not take computer scrap paper home; and
 - do not allow unauthorised use of computer equipment issued by the Company.
- Always ensure that data is input correctly. Do not delay in inputting new data when available.
- Do not make any oral or written reference to personal data held by the Company about any individual except to Employees of the Company who need the information for their work or a registered recipient.
- Take great care to establish the identity of any person asking for personal information. Make sure that the person is entitled to receive the information.
- If an Employee is asked by an individual to provide details of their personal information held by the Company, the Employee should ask that they put their request in writing and send it to our HR Manager. If the request is in writing pass it immediately to our HR Manager.
- Do not use personal information for any purpose other than your work for the Company.
- If the Employee is in doubt about any matter to do with data protection do not guess - refer the matter to your manager immediately.

Whistleblowing

This policy will in no way affect the rights of disclosure of information under the Public Interest Disclosure Act 1998

Signed: A. Dalrymple
(Andy Dalrymple, Managing Director)

Date: 7/1/19

Signed: [Signature]
(Mark Wilson, Contracts Director)

Date: 7/1/19

PRIVACY NOTICE

WHAT IS THE PURPOSE OF THIS DOCUMENT?

Mackenzie Construction is committed to protecting the privacy and security of your personal information.

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 General Data Protection Regulation (GDPR).

It applies to all employees, workers and contractors.

Mackenzie Construction is a "data controller". 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 employees, workers and contractors. 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 may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence.

- 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).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage if on site
- Information about your use of our information and communications systems.
- Photographs.

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

- [Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.]
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We typically collect personal information about employees, workers and contactors 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 [or for official purposes].

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 process your personal information are listed below. [We have indicated by [asterisks] the purpose or purposes for which we are processing or will process your personal information, as well as indicating which categories of data are involved.]

- 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. **
- Paying you and, if you are an employee, deducting tax and National Insurance contributions. **
- Providing the following benefits to you: Private Healthcare if applicable. Occupational Health Support ***

- Liaising with your pension provider. ***
- Administering the contract we have entered into with you. *
- Business management and planning, including accounting and auditing. ***
- Conducting performance reviews, managing performance and determining performance requirements.*
- General business communications
- Making decisions about salary reviews and compensation. *
- Assessing qualifications for a particular job or task, including decisions about promotions. ***
- Gathering evidence for possible grievance or disciplinary hearings. **
- 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 employees, workers and contractors, including accidents at work. **
- Ascertaining your fitness to work. ***
- Managing sickness absence. *
- Complying with health and safety obligations. *
- To prevent fraud. ***
- To monitor your use of our information and communication systems to ensure compliance with our IT policies. ***
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. ***
- 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 GDPR 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 GDPR.
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 AS AN EMPLOYER

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 may 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.

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 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 envisage that we will hold information about criminal convictions.

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

When required, to obtain clearance to work with certain clients. In particular M.O.D

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 may 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: monthly payroll, pension administration, benefits provision and administration, IT services, training.

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, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

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.

TRANSFER OF DATA OUTSIDE THE EU

The Company will transfer the personal information to the following country outside the EU (Mauritius) for the following reasons: processing monthly payroll. There is not an adequacy decision by the European Commission in respect of that country. This means that the country to which the Company transfers data are not deemed to provide an adequate level of protection for personal information.

However, to ensure that personal information does receive an adequate level of protection the Company has put in place the following appropriate measure[s] to ensure that personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection: incorporating standard contractual clauses (which the European Commission has decided offer sufficient safeguards) in to our agreement with the payroll provider.

DATA SECURITY

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

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. Details of these measures may be obtained from HR.

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. 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 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.

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 our HR Manager 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.

DATA PROTECTION & PRIVACY NOTICE POLICY

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 our HR Department. 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.

DATA PROTECTION OFFICER

We have appointed a Data Privacy Manager to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact Alison Irwin (Quality & IT Co-ordinator). 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.

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.

Signed: A. Dalrymple
(Andy Dalrymple, Managing Director)

Date: 7/1/19

Signed: [Signature]
(Mark Wilson, Contracts Director)

Date: 07/01/19