MORRIS GROUP

PRIVACY POLICY

APRIL 2023

PRIVACY POLICY

This policy has been adopted by Morris & Company (Shrewsbury) Limited (Company number 5041054), Morris & Company Limited (Company number 0185693), Morris Property Limited (Company number 3033776), Morris Site Machinery Limited (Company number 1063091) and all other subsidiaries of Morris & Company (Shrewsbury) Limited (Company number 5041054) from time and time together referred to as the Morris Group.

Morris & Company (Shrewsbury) Limited is required to gather and store information about You. We take Our responsibility for data privacy very seriously. This policy explains how data will be gathered, handled and stored. It also details the rules and Your rights regarding privacy of information. This policy sets out how the Company will collect and deal with the data You provide to Us during the course of Your contract with Us. This policy should be read alongside other key policies. In particular, You should also read Our Information Governance, social media, email and internet use policies.

THE FOLLOWING TERMINOLOGY WILL BE USED THORUGHOUT THE POLICY:

"We", "Us", "Our", "Morris Group" and **"Company"** means Morris & Company (Shrewsbury) Limited including Morris Property Limited, Morris Site Machinery Limited, Morris & Company Limited, their subsidiaries and any other Company within the Morris Group or any trading division of Morris & Company (Shrewsbury) Limited.

"You", "Your" and **"Data subject"** means current and former employees, applicants, workers, volunteers, apprentices, partners and consultants of the Company.

"DPO" means the Data Protection Officer appointed by the Company.

"ICO" means the Information Commissioner's Office (address).

"Personal Data" for this purpose means any information relating to an identified or identifiable person.

"Special Categories of Data" means Personal Data relating to:

- Your racial or ethnic origin;
- Your political opinions;
- Your religious or philosophical beliefs;
- Your membership of a trade union;
- Your physical or mental health or condition;
- Your sexual life;
- Any offence committed or alleged to have been committed by You;
- Any proceedings for any offence committed or alleged to have been committed by You, the disposal of such proceedings or the sentence of any court in such proceedings;
- Your genetic data;
- Your biometric data where processed to uniquely identify You.

"Processing" means any operation or set of operations which is performed on Personal Data such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, restriction, erasure or destruction.

1. WHY THIS POLICY EXISTS

1.1 We are committed to protecting and respecting Your privacy and this policy sets out the basis on which any Personal Data We collect, or that is provided to Us, will be processed by all those who handle the data.

This policy helps ensure We:

a) Protect You and the Company from harm
b) Comply with General Data Protection Regulation (GDPR) and follow good practice
c) Reduces the security and business risks faced by the Company
d) Are clear why We are permitted to hold and use Person Data about You
e) Let You know how You are permitted to use information
f) Satisfy Our legal obligations regarding privacy

2. SCOPE

2.1 This policy applies to all Our employees, contractors and volunteers who gather, handle, process or remove data. It applies no matter what the information is, as long as it is identifiable in some way to You.

This policy does not apply to any information which has been anonymised or pseudonymised and is therefore untraceable and unidentifiable.

3. GENERAL DATA PROTECTION REGULATION (GDPR)

3.1 The GDPR includes six data protection principles which organisations must be able to demonstrate they have followed in respect of any Personal Data they handle. We will ensure all data collected handled will be:

a) Processed lawfully, fairly and transparently
b) Collected for specified, explicit and legitimate purposes
c) Adequate, relevant and limited to what is necessary
d) Accurate and, where necessary, kept up to date
e) Kept for no longer than is necessary where data subjects are identifiable
f) Processed securely and protected against accidental loss, destruction or damage.

4. THE INFORMATION WE COLLECT

4.1 The Personal Data that may be provided to the Company can include, but is not limited to:

a) Name
b) Home address
c) Email address
d) Phone Numbers
e) Qualifications
f) Career history
g) Emergency contact information
h) Financial and credit card information
i) Personal description
j) Photograph
k) Special Categories of Data (as detailed above)

4.2 This information can be provided in the form of, but not limited to:

a) Forms filled out in relation to your role
b) Correspondence by email, phone or otherwise
c) Information provided to form a contract with the Company

4.3 We are lawfully bound to only process data for specific reasons and for a specific amount of time. However, there is occasionally lawful ground for holding data for an extended period, i.e. collecting and holding bank details to pay salary as part of an employment contract.

Data includes any of the above information processed from any source, and held by the company in either electronic or paper, particularly Personal Data held or processed by the Company on any of the following (but not limited to):

a) Computers
b) Mobile devices such as laptops, phones and tablets
c) Email
d) Media
e) Websites
f) Networks
g) Hard copy media

4.4 Under the GDPR, when We process Personal Data or special categories of data, it will be dealt with under at least one of the following conditions:

a) **Consent –** You have consented to the processing.
b) **Contractual –** processing is necessary for the performance of a contract with You or to take steps to enter into a contract.
c) **Legal obligations –** processing is necessary for Us to comply with a legal obligation.
d) **Vital interests –** processing is necessary to protect You or someone else's vital interests.
e) **Public tasks –** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the business.
f) **Legitimate interests –** processing is necessary for purposes of legitimate interests of the business or a third party, except where those interests are overridden by Your interests, rights or freedoms.

4.5 When processing Special Categories of Data, if the data is not considered necessary for carrying out the obligations as an employer, We will obtain additional consent for You for this processing. This will be assessed on a case by case basis.

5. HANDLING INFORMATION

5.1 We will use the information given to Us:

a) to carry out Our obligations arising from any contracts entered into and to provide the information and services that are required from Us;
b) to notify You about changes within the Company where relevant;
c) to write to You in relation to roles within the Company, if necessary.

5.2 Your data will be shared as required by regulatory bodies or in accordance with legal requirements.

DISCLOSURE OF YOUR INFORMATION

5.3 Data will never be shared informally. When access to confidential information is required, You can request this from Your manager.

Sharing of information to third parties will only occur if We are under a duty to disclose or share Your Personal Data to comply with any legal obligation, or to protect the rights, property, or safety of the Company, Our customers, employees or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

5.4 Nothing in this policy shall derogate from the Company's entitlement to make a "qualifying disclosure" as defined by the Public Interest Disclosure Act 1998 (as amended or replaced from time to time) or prevent the Company from making any disclosure required by law.

HOW/WHERE WE STORE PERSONAL DATA

5.5 We will only keep Personal Data for as long as is strictly necessary, with regard to the original purpose for which it was processed. In some cases, We will be legally obliged to keep the data for a set period.

When data is stored on paper, it will be kept in a secure cabinet where only authorised personnel have access.

5.6 Data will be stored electronically using Our secure HR system called Select HR. This is a secure platform where You will have access to Your Personal Data.

6. EMAIL AND INTERNET USAGE GUIDELINES

6.1 When processing Your data, the Company will not send Personal Data to external emails without ensuring the data is secure and the Company has the appropriate authorisation. Security may be in the form of encryption, pseudonym or by other means. Emails between company user account are encrypted end to end and are therefore secure. For more information on this, please contact the DPO and refer to Our email and internet policies.

Data may be sent within the Company if necessary and there is a lawful basis for the transfer of the information.

6.2 Only people who have been authorised to use Our email facilities may do so. Authorisation is usually provided by Your line manager or a Company Director. It is typically granted when a new employee joins the Company and is assigned their login details for the Company IT systems.

7. MOBILE DEVICES

7.1 We reserve the right to monitor use of Company Mobile Devices, the internet on Company time, and to examine systems and review the data stored in those systems. These examinations or monitoring will only be carried out by authorised staff of the Company.

Additionally, all online data written, sent or received through the Company's computer systems is part of official Company records. The Company can be legally compelled to show that information to law enforcement agencies or other parties.

8. YOUR RIGHTS

8.1 Your rights under GDPR are as follows:

1) The right to be informed – The right to be informed of why and how Your data is being processed. Any information given must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
2) The right of access – You have the right to be aware of all information We hold on You. For this reason, you can request access to this data by making a Subject Access Request. Please see "Access to Information" overleaf and refer to the Information Governance policy for more information and Subject Access Requests.
3) The right to rectification – The right to rectify any incomplete or inaccurate information We hold on You.
4) The right to erasure/to be forgotten – You request for any information held on You to be erased. This request will be granted as long as there is no lawful or legitimate reason for the data to continue to be held. If a legitimate reason is found and the Company were to refuse this request, You will be informed.
5) The right to restrict processing – You have the right to suppress further processing if You have previously contested the accuracy or incompleteness of Your data the We hold on You.
6) The right to data portability – The right to receive data in a structured, commonly used and machine-readable format. You also have the right to have this data transported to another controller without hindrance if it is carried out by automated means.
7) The right to object – If the Company is processing information for legal reasons or for the Company's legitimate interests then You have the right to object on "grounds relating to Your particular situation". This objection must be in writing to either Your line manager or

the HR department stating clear reasons for the objection. This objection may be refused if legitimate reasons outweigh Your interests.

8) The right not to be subject to automated decision making including profiling – The right not to be part of a decision when it is based on automated processing and it therefore produces a legal effect or a similarly significant effect on You. This right does not apply if the decision is necessary for purposes of the performance of a contract between You and the Company.

MARKETING PURPOSES

8.2 You have the right to ask us not to process Your Personal Data for marketing purposes. We will inform You (before collecting the data) if We intend to use it for such purposes or if We intend to disclose the information to any third party for these purposes. You can exercise Your right to prevent such processing by checking certain boxes on the forms We use to collect the data. You can also exercise the right at any time by contacting Us at HR@morrisandco.com.

Our site may, from time to time, contain links to and from the websites of partner networks, advertisers and affiliates. Please note that these websites have their own privacy policies and that We do not accept any responsibility for or liability under these policies.

ACCESS TO INFORMATION

8.3 You have the right to access information held on You. This right of access can be exercised in accordance with the GDPR. For more information, refer to the Information Governance Policy.

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer at DPO@morrisandco.com, or made in writing to;

The Data Protection Officer
Morris and Company
Welsh Bridge
Shrewsbury
Shropshire
SY3 8LH

WITHDRAWING CONSENT

8.4 If You wish to withdraw consent at any time, You will need to contact the Data Protection Officer as above. We will make it easy for You to withdraw Your consent, where possible, at any time. We will act on withdrawals of consent as soon as We can and will not penalise individuals who wish to withdraw consent.

9. PERSONAL DATA BREACHES

DATA PROTECTION RISKS

9.1 This policy helps us to protect the Company from some very real data security risks, including:

a) **Breaches** of confidentiality. For instance, information being given out inappropriately. *See Our Data Breach Policy.*

b) **Failing to offer choice.** For instance, all individuals should be free to choose how the Company uses data relating to them.

c) **Reputational damage.** For instance, We could suffer if hackers successfully gained access to sensitive data.

PERSONAL DATA BREACHES

9.2 A Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Please read Our separate *Data Breach Policy*.

9.3 If You discover a data breach or You think there is the potential for a data breach (including those that appear to be insignificant), You have duty to report this to the Data Protection Officer (DPO) **immediately, or at the earliest possible opportunity** (if discovered out of hours, no later than the next working day).

HOW TO REPORT A DATA BREACH

9.4 Details of what constitutes a data breach, and detailed guidance on the reporting process are out in Our *Data Breach Policy*. You will be required to submit a *Data Breach Incident Report Form*, which is attached to the Data Breach Policy. For help accessing the policy please see Yours manager or speak to HR on 01743 232005.

Where the breach is likely to adversely affect the Personal Data or privacy of the data subject/s, the DPO must report it to the supervisory authority, no later than 72 hours of the initial discovery of the breach.

10. CONTACT

10.1 If You have any questions regarding this policy, please contact the DPO at DPO@morrisandco.com. Alternatively, please call the HR Department on 01743 232005.

11. POTENTIAL SANCTIONS

11.1 Knowingly breaching this Privacy Policy is a very serious matter. If You do so You may be subject to disciplinary action up to and including termination of employment. You could also be held personally liable for violating this policy.

11.2 Under the GDPR, You now have the personal liability if a significant breach were to take place. Where appropriate, the Company will involve the police or other law enforcement agencies in relation to breaches of this policy.