GDPR Policy and Privacy Notice.

Pave Aways Limited,
Avenue Mill,
Knockin,
Oswestry,
SY10 8HQ
01691 682111

PRIVACY POLICY

1. INTRODUCTION

1.1. The Company wholly recognises the fundamental right to privacy, security and data protection for our customers, employees, workers, contractors, suppliers, and partners.

1.2. This Privacy Policy sets out how the Company handles the Personal Data of our customers, clients, suppliers, employees, workers and other third parties.

1.3. This Privacy Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients, suppliers, shareholders, website users or any other Data Subject. However, it does not set terms or conditions of employment or otherwise form part of an employment contract.

1.4. This Privacy Policy applies to all Personnel. You must read, understand, and comply with this Privacy Policy when Processing Personal Data on our behalf and attend training on its requirements as directed. This Privacy Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Privacy Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Policy. You must also comply with all such Related Policies and Guidelines. Any breach of this Privacy Policy by an employee may result in disciplinary action.

1.5. This Privacy Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients, or regulators without prior authorisation from the Data Privacy Manager.

2. INTERPRETATION

Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company: Pave Aways Limited

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Criminal Records Information: personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Data Controller of all Personal Data relating to Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Privacy Manager (DPM): the data protection manager who has responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity, or availability of Personal Data or the physical, technical, administrative, or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure, or acquisition, of Personal Data is a Personal Data Breach.

Personnel: all employees, workers, contractors, agency workers, consultants, directors, or other personnel engaged by or on behalf of the Company.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notices: separate notices (sometimes otherwise referred to as fair processing notices) setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or a website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies and Guidelines: The Company's policies, guidelines, operating procedures or processes related to this Privacy Policy from time to time and designed to protect Personal Data, available from the HR Department.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

UK GDPR: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679).

3. SCOPE

3.1. We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to £17.5 million) or 4% of total annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

3.2. All levels of management are responsible for ensuring all Personnel comply with this Privacy Policy and need to implement appropriate practices, processes, controls, and training to ensure such compliance.

3.3. The DPM is responsible for overseeing this Privacy Policy and, as applicable, developing Related Policies and Guidelines. That post is held by Jane Harvey, HR Manager telephone: 01691 682 111 email: jane.harvey@paveaways.co.uk

3.4. Please contact the DPM with any questions about the operation of this Privacy Policy or the UK GDPR or if you have any concerns that this Privacy Policy is not being or has not been followed. In particular, you must always contact the DPM in the following circumstances:

3.4.1. if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company).

3.4.2. if you need to rely on Consent and/or need to capture Explicit Consent.

3.4.3. if you need to draft Privacy Notices.

3.4.4. if you are unsure about the retention period for the Personal Data being Processed.

3.4.5. if you are unsure about what security or other measures you need to implement to protect Personal Data.

3.4.6. if there has been a Personal Data Breach.

3.4.7. if you are unsure on what basis to transfer Personal Data outside the EEA.

3.4.8. if you need any assistance dealing with any rights invoked by a Data Subject.

3.4.9. whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for.

3.4.10. if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making.

3.4.11. if you need help complying with applicable law when carrying out direct marketing activities; or

3.4.12. if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1. We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

4.1.1. processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

4.1.2. collected only for specified, explicit and legitimate purposes (Purpose Limitation).

4.1.3. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

4.1.4. accurate and where necessary kept up to date (Accuracy).

4.1.5. not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

4.1.6. processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

4.1.7. not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

4.1.8. made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4.2. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1. Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process, and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but to ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The UK GDPR allows Processing for specific purposes, some of which are set out below:

5.1.1. the Data Subject has given his or her Consent.

5.1.2. the Processing is necessary for the performance of a contract with the Data Subject.

5.1.3. to meet our legal compliance obligations.

5.1.4. to protect the Data Subject's vital interests; and/or

5.1.5. to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

You must identify and document the legal ground being relied on for each Processing activity.

5.2. Consent

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly, either by a statement or positive action, to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data, for Automated Decision-Making and for cross border data transfers. Usually, we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Categories of Personal Data. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

5.3. Criminal Records Information

Criminal records information will be processed in accordance with our Criminal records information policy.

5.4. Transparency (notifying data subjects)

The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Data Controller and DPM, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis, which contemplates our proposed Processing of that Personal Data.

6. PURPOSE LIMITATION

6.1. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

6.2. You cannot use Personal Data for new, different, or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION

7.1. Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed.

7.2. You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

7.3. You may only collect Personal Data that you require for your job duties. Do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

7.4. You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

8. ACCURACY

8.1. Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

8.2. You will ensure that the Personal Data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. STORAGE LIMITATION

9.1. Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.2. You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

9.3. The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held unless a law requires such data to be kept for a minimum time. You must comply with the Company's guidelines on Data Retention.

9.4. You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

9.5. You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

10.1. Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

10.1.1. **Confidentiality** means that only people who have a need to know and are authorised to use the Personal Data can access it.

10.1.2. **Integrity** means that Personal Data is accurate and suitable for the purpose for which it is processed.

10.1.3. **Availability** means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

10.2. Reporting a Personal Data Breach

The UK GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator, and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPM. You should preserve all evidence relating to the potential Personal Data Breach.

11. TRANSFER LIMITATION

11.1. We do not transfer your personal data outside the UK.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

12.1. Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

12.1.1. withdraw Consent to Processing at any time.

12.1.2. receive certain information about the Data Controller's Processing activities.

12.1.3. request access to their Personal Data that we hold.

12.1.4. prevent our use of their Personal Data for direct marketing purposes.

12.1.5. ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data.

12.1.6. restrict Processing in specific circumstances.

12.1.7. challenge Processing which has been justified on the basis of our legitimate interests or in the public interest.

12.1.8. request a copy of an agreement under which Personal Data is transferred outside of the EEA.

12.1.9. object to decisions based solely on Automated Processing, including profiling (ADM).

12.1.10. prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else.

12.1.11. be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms.

12.1.12. make a complaint to the supervisory authority; and

12.1.13. in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the DPM.

13. ACCOUNTABILITY

13.1. Technical and organisational measures to ensure compliance.

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

13.1.1. appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy.

13.1.2. implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects.

13.1.3. integrating data protection into internal documents including this Privacy Policy, Related Policies and Guidelines, and Privacy Notices.

13.1.4. Regularly training Personnel on the UK GDPR, this Privacy Policy, Related Policies and Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Personnel; and

13.1.5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

13.2. Record keeping

The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company's document control guidelines.

These records should include, at a minimum, the name and contact details of the DPM, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

13.3. Training and audit

We shall ensure all Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all and any mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

13.4. Privacy by Design

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

13.4.1. the state of the art.

13.4.2. the cost of implementation.

13.4.3. the nature, scope, context, and purposes of Processing; and

13.4.4. the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

13.5. Data Protection Impact Assessment (DPIA)

Data controllers must conduct DPIAs in respect to high-risk Processing.

You should conduct a DPIA when implementing major system or business change programs involving the Processing of Personal Data including:

13.5.1. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes).

13.5.2. Automated Processing including profiling and ADM.

13.5.3. large scale Processing of Special Categories of Personal Data; and

13.5.4. large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

13.5.5. a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate.

13.5.6. an assessment of the necessity and proportionality of the Processing in relation to its purpose.

13.5.7. an assessment of the risk to individuals; and

13.5.8. the risk mitigation measures in place and demonstration of compliance.

You must comply with the Company’s guidelines on DPIA and Privacy by Design.

13.6. Automated Processing (including profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

13.6.1. a Data Subject has Explicitly Consented.

13.6.2. the Processing is authorised by law; or

13.6.3. the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of Personal Data are being processed, then the grounds listed at 13.6.2 or 13.6.3 will not be allowed but such Special Categories of Personal can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Please contact the DPM if you engage or intend to engage in any data Processing activity that involves profiling or ADM.

Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text, or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Please contact the DPM if you engage or intend to engage in direct marketing to customers.

Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of the Company if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

13.6.4. they have a need to know the information for the purposes of providing the contracted services.

13.6.5. sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained.

13.6.6. the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.

13.6.7. the transfer complies with any applicable cross border transfer restrictions; and

13.6.8. a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

You must comply with the Company's guidelines on sharing data with third parties.

14. CHANGES TO THIS PRIVACY POLICY

We reserve the right to change this Privacy Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Privacy Policy.

This Privacy Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

PAVE AWAYS LTD

DATA PROTECTION PRIVACY NOTICE - employers, workers and contractors

This notice explains what personal data (information) we hold about you, how we collect it, and how we use and may share information about you during your employment and after it ends. We are required to notify you of this information under data protection legislation. Please ensure that you read this notice (sometimes referred to as a 'privacy notice') and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

Pave Aways Ltd is a 'data controller' and gathers and uses certain information about you.

We will comply with the data protection principles when gathering and using personal information, as set out in our Data Protection Policy.

The table set out in schedule 1 summarises the information we collect and hold, how and why we do so, how we use it and with whom it may be shared.

We may also need to share some of the categories of personal information set out in schedule 1 with other parties, such as external contractors and our professional advisers and potential purchasers of some or all of our business or on a re-structuring. Usually, information will be anonymised, but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

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

Information may be held at our offices and third party agencies, service providers, representatives and agents as described above.

We keep your information during and after your employment or other engagement for no longer than is necessary for the purposes for which the personal information is processed. Further details on this are available in our Data Retention Policy, which is available from the HR Manager. However, we also have regard to legal risk and may keep records for up to 7 years (and in some instances longer) after your employment or work with us has ended. 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.

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 the HR Manager in writing at jane.harvey@paveaways.co.uk

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

6.5 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.

We have appropriate security measures in place to prevent personal information from being accidentally lost or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

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

We hope that our HR Manager can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

We reserve the right to update this 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.

Schedule 1

About the information we collect and hold

The information we collect	How we collect the information	Why we collect the information	How we use and may share the information
Your name, contact details (i.e. address, home and mobile phone numbers, email address) and emergency contacts (i.e. name, relationship and home and mobile phone numbers) ☐	From you	To enter into/perform our contract with you Legitimate interest: to maintain employment records and good employment practice	To enter into/perform our contract with you
Details of salary and benefits, bank/building society, National Insurance and tax information, and your date of birth ☐	From you	To perform our contract with you, including making payments to you and providing benefits Legitimate interests: to maintain employment or other records and to comply with legal, regulatory and corporate governance obligations and good practice	To ensure you receive the correct pay and benefits Information shared with our payroll administrators and with HM Revenue & Customs (HMRC)
Details of your spouse/partner and any dependants ☐	From you	To perform our contract with you including employment-related benefits, e.g. private medical insurance, life assurance and pension. Emergency contact details.	To ensure you receive the correct pay and benefits Information shared with our payroll administrators and with HM Revenue & Customs (HMRC)
Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information ☐	From you and, where necessary, the Home Office	To enter into/perform our contract with you To comply with our legal obligations Legitimate interest: to maintain employment records	To carry out right to work checks Information may be shared with the Home Office
Driving licence information ☐	From you	**T**o perform our contract with you To comply with our legal obligations To comply with the terms of our insurance	To ensure that you have a valid driving licence Information may be shared with our insurer

Details of your pension arrangements, and all information included in these and necessary to implement and administer them ☐	From you, from our pension administrators and (where necessary) from your own pension fund administrators	To perform the employment contract including employment-related benefits To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	To administer your pension benefits AND/OR to comply with our auto-enrolment pension obligations Information shared with our pension administrators and with HMRC
Information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health) ☐	From you, from your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators	To perform our contract with you including regarding any employment-related benefits To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good practice, to ensure safe working practices	To maintain employment records, to administer sick pay entitlement, to follow our policies and to facilitate employment-related health and sickness benefits To comply with our legal obligations to you as your employer Information shared with your doctors, with medical and occupational health professionals we engage and with our insurance benefit administrators For further information, see * below
Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs	From you	To comply with our legal obligations and for reasons of substantial public interest (equality of opportunity or treatment)	To comply with our equal opportunities monitoring obligations and to follow our policies For further information, see * below
Criminal records information, including the results of Disclosure and Barring Service (DBS) checks ☐	From you and the DBS	To perform our contract with you To comply with our legal obligations	To carry out statutory checks Information shared with DBS

		For reasons of substantial public interest (preventing or detecting unlawful acts, suspicion of terrorist financing or money laundering in the regulated sector and protecting the public against dishonesty)	and other regulatory authorities as required For further information, see * below
Information on grievances raised by or involving you	From you, from complainants, from witnesses and from managers or third parties we may engage in relation to investigating and/or presiding over the grievance procedure	To perform the employment contract To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good practice	For staff administration, to follow our policies and to deal with grievance matters Information shared with relevant employees or other complainants or witnesses, HR personnel and with employees or third parties we may engage
Information on conduct issues involving you	From you, from complainants, from witnesses and from managers or third parties we may engage in relation to investigating and/or presiding over a disciplinary procedure	To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	For staff administration and assessments, to follow our policies, to monitor staff performance and conduct and to deal with disciplinary matters Information shared with relevant witnesses, HR personnel and with employees or third parties we may engage
Details of your appraisals and performance reviews	From you, from other employees and from third parties we may engage in relation to the appraisal/performance review process	To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	For staff administration and assessments, to follow our policies, to monitor staff performance Information shared with relevant managers, HR personnel and with third parties we may engage

Details of your performance management/improvement plans (if any)	From you, from other employees and **from managers or third parties we may engage in relation to any performance management process**	To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	For staff administration and assessments, to follow our policies and to monitor staff performance Information shared with relevant managers, HR personnel and with third parties we may engage
Details of your time and attendance records	From you and from Timekeeper	To perform the employment contract Legitimate interest: to monitor and manage staff access to our systems and facilities and to record staff absences	For payroll and staff administration and assessments, to follow our policies and to monitor staff attendance Information shared with relevant managers, HR personnel and with third parties we may engage, and with our payroll administrators
Information in applications you make for other positions within our organisation	From you	To enter into/perform our contract with you To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good practice	To process the application Information shared with relevant managers, HR personnel and with third parties we may engage
Information about your use of our IT, communication and other systems	Automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, remote access systems, email and instant messaging systems, intranet and Internet facilities, telephones, voicemail, mobile phone records	Legitimate interests: to monitor and manage staff access to our systems and facilities to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel and with consultants we may engage

		to ensure our business policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, recording transactions, training and quality control to ensure that commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with for security vetting and investigating complaints and allegations of criminal offences to prevent unauthorised access and modifications to our systems as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	For further information, see ** below
Details of your use of business-related social media, such as LinkedIn	From relevant websites and applications	Legitimate interests: to monitor and manage staff access to our systems and facilities to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage to ensure our business policies, such as those concerning security	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel and with consultants we may engage For further information, see ** below

		and internet use, are adhered to for operational reasons, such as maintaining employment records, recording transactions, training and quality control to ensure that commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with **[**for security vetting and investigating complaints and allegations of criminal offences**]** as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	
Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur)	From relevant websites and applications	Legitimate interests: to monitor and manage staff access to our systems and facilities to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage to ensure our business policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, recording transactions, training and quality control	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel and with consultants we may engage For further information, see ** below

		to ensure that commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with **[**for security vetting and investigating complaints and allegations of criminal offences**]** as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	
Details in references about you that we give to others	From your personnel records, our other employees	To perform the employment contract To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	To provide you with the relevant reference To comply with legal/regulatory obligations Information shared with relevant managers, HR personnel and the recipient(s) of the reference
If you drive a work vehicle that you have been notified is installed with a tracking device, the location [and speed] of your work vehicle (if private use of the vehicle is permitted, then only during working hours, unless the theft or otherwise loss of the vehicle is known or suspected)	From a tracking device	Legitimate interests: to monitor and facilitate the efficient distribution of resources to ensure that our policies regarding vehicle use are complied with to maintain the security of vehicles and their contents and the safety of their operators	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel and, if required, our insurers For further information, see ** below

You are required (by law or under the terms of your contract of employment, or in order to enter into your contract of employment) to provide the categories of information marked '☐' above to us to enable us to verify your right to work and

suitability for the position, to pay you, to provide you with your contractual benefits and to administer statutory payments such as statutory sick pay (SSP). If you do not provide this information, we may not be able to employ you, to make these payments or provide these benefits.

***** Further details on how we handle sensitive personal information and information relating to criminal convictions and offences are set out in our company handbook.

****** Further information on the monitoring we undertake in the workplace and how we do this is available from the HR Manager.

Signed by Steven Owen, Managing Director



Dated; 02/09/26
Review date: 02/09/27