VERDANT

Privacy Policy

What is a Privacy Notice?

A privacy notice is a statement explaining how personal and confidential information about candidates, corporate clients, visitors, and staff is collected, used and shared within Verdant Recruitment (referred to as “We, “Our” or “Us”) Different organisations use different names for privacy notices, and it can sometimes be referred to as a privacy statement, a fair processing notice or a privacy policy.

What is Verdant Recruitment and what does it do?

Verdant Recruitment is a recruitment agency based in Suffolk, United Kingdom and is sourced by its clients to fill roles it has been asked to seek.

Everything Verdant Recruitment does is underpinned by our core values:

- Candidate Experience
- Collaborative partnerships
- Transparency
- Relentless innovation
- Human centred

Why have a privacy notice for candidates, corporate clients, visitors, and staff?

Verdant Recruitment would like to demonstrate its commitment to openness and accountability. We recognise the importance of protecting personal and confidential information in all that we do to ensure that we meet our legal responsibilities and other duties, including compliance with the following:

Data Protection Act (DPA)

General Data Protection Regulation (GDPR)

How we collect your information?

Your information could be collected in several ways by us. This maybe through our services, for example job applications, on the website, on social media, or in person, for example on the phone or in branch. Or from third-party job boards where you have registered your Curriculum Vitae (CV) for the purposes of finding work.

What information do we collect about you?

The information that we collect is provided by you and may include details such as:

- Personal information
- name, address, telephone, email date of birth and next of kin
- copies of driving licence, passport, and proof of current address, such as bank statements and council tax bills
- evidence of how you meet the requirements of a job, including CV and reference checks
- evidence of your right to work in the UK and immigration status

VERDANT

- bank details, tax and NI number for processing payments
- other information relevant to customer surveys and/or offers
- Guest / visitors to one of your sites

Special Category information

- Diversity and equal opportunities monitoring information – this can include information about your race or ethnicity, religious beliefs, sexual orientation, disability
- Information about your health, including any medical needs or conditions

For some jobs we may require asking you to.

- provide person information of individuals who can provide references
- provide details of any criminal convictions (including a DBS certificate or update service details)

Why do we collect information?

We collect personal and confidential information about you to support you in the recruitment and employment process. It is important that we provide the best experience while meeting your needs.

How do we use your information and why is this important?

We use your personal information to deliver the best experience to help understand your and where it is necessary to meet our obligations which may include:

to provide a recruitment service to you and to facilitate the recruitment process

to assess data about you against vacancies which we believe may be suitable for you

to send your information to clients in order to apply for jobs, to assess your eligibility for jobs or to process you for work (including pre-contract, during and post-contract)

to improve our client and recruitment experience and to make our services more valuable to you (including gathering your feedback and tailoring our website, applications and our group companies' websites when you log on to enrich your personal online experience)

to respond to questions and enquiries

- To engage third parties where we have retained them to provide services that we, you or our client have requested including payroll services, references, qualifications and criminal reference checking services, verification of the details you have provided from third party source, psychometric evaluation or skill tests
- To inform third parties, regulatory or law enforcement agencies if we believe in good faith that we are required by law to disclose it in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law or order of a court of competent jurisdiction, or in connection with legal proceedings. Please also note we may retain and share details of incidents where threats have been made to the safety and security of our members of staff with any law enforcement agencies when needed. This may also result in individuals being barred from using our services

VERDANT

- To use your information on an anonymised basis to monitor compliance with our equal opportunities policy

How do we keep your information safe and maintain confidentiality?

The GDPR and Data Protection Act has strict principles governing our use of information and our duty to ensure that it is kept safe and secure. Your information may be stored using electronic or paper records, or a combination of both. All our records are restricted so that only authorised individuals have access to them. Restricted access might be using technology or other environmental safeguards.

Sharing with other organisations

Personal information you provide to us will be made available to clients and our processors. By providing your information to us you have agreed to our terms and conditions that you have consented through the sign-up process. Implied consent under certain conditions maybe applied for example:

- Applying directly to jobs via independent jobs boards (candidates or staff)
- Processing information for the purpose of processing payments (salary)

We will share your information to other agencies or organisations who are involved in the recruitment process, who may be the data controller and/or processor of your information.

We may be required to share your personal information for “Legitimate interests” which may include (but not limited to):

- To assess your information about you with current vacancies which we believe may be suitable for you
- To send your information to clients in order to apply for jobs, to assess your eligibility for jobs or to process you for work (including pre-contract, during and post-contract)
- To engage third parties where we have retained them to provide services that we, you or our client have requested including payroll services, references, qualifications and criminal reference checking services, verification of the details you have provided from third party source, psychometric evaluation or skill tests
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as we currently do, which can also extend to consents for marketing communications
- To inform third parties, regulatory or law enforcement agencies i required by law to disclose it in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law or order of a court of competent jurisdiction, or in connection with legal proceedings.
- To use your information on an anonymised basis to monitor compliance with our equal opportunities policy

- To improve our customer service and to make our services more valuable to you (including gathering your feedback via email and tailoring our website, applications and our group companies' websites when you log on to enrich your personal online experience)
- Audit, Research, and Artificial Intelligence ("AI")

Audit

Mandatory audits are undertaken to ensure we are process, store and share your data appropriately. We are unable to apply data opt-outs to audits as these are mandatory and regulatory requirements.

Research

We will share your anonymised information for statistical analysis. Once the data has gone through the anonymised process it will no longer be classified as personal information and is exempt from GDPR & the Data Protection Act. We are unable to apply data opt-outs as the data would not be able to identify a specific individual.

Artificial Intelligence ("AI")

We are always looking at ways to innovate to improve our efficiency to delivery you the best experience. AI maybe used in the future and if we to use your information where you are formally identified they we ask for your consent.

We may use anonymised data for the use of AI as this will no longer be classified as personal information and is exempt from GDPR & the Data Protection Act. We are unable to apply data opt-outs as the data would not be able to identify a specific individual.

Do you have the right to withhold or withdraw your consent for information sharing?

You have the right to refuse (or withdraw) consent to your information being shared at any time. This may be referred to as 'opt-out'. If you choose to prevent your information being disclosed it may restrict the services we provide to you, which may mean we may not be able to use our services. The possible consequences of withholding your consent will be fully explained to you at the time should this situation occur.

Where do we store your information?

Verdant Recruitment securely stores your information electronically and occasionally in paper form. We use different systems depending on the process we require to undertake and are subject to change:

System Purpose

- A product for managing customer and candidate data, and supporting the recruitment process
- Accounting software: Company accounts, Invoice, manage payroll a and Pensions
- Specialist software for the staffing and recruitment industries to manage temporary worker payroll and invoicing
- LinkedIn: Job seekers posting CVs in response to job adverts
- Indeed, CV Library or similar. To review current job opportunities

VERDANT

How long we keep information about you?

Your personal data will be kept in line with statutory and recommend retention periods:

Statutory record retention period

Record type: Statutory retention period

Accident books, accident records/reports: 3 years from the last entry (or until any younger person involved in the accident reaches 21).

Accounting records: 3 years for private companies, 6 years for public limited companies.

Coronavirus furlough records: N/A Verdant was formed October 2024

First aid training: 6 years after employment.

Fire warden training: 6 years after employment.

Health and Safety representatives and employees' training: 5 years after employment.

Income tax and NI returns, income tax records and correspondence with HMRC: Not less than 3 years after the end of the relevant financial year.

Medical records and details of biological tests under the Control of Lead at Work Regulations :40 years from the date of the last entry.

Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) : 40 years from the date of the last entry.

Medical records under the Control of Asbestos at Work Regulations :40 years from the date of the last entry (medical records); 4 years from the date of issue (medical examination certificates).

Medical records under the Ionising Radiations Regulations 1999: Until the person reaches 75 years of age, but in any event for at least 50 years.

National minimum wage records :6 years after the end of the pay reference period following the one that the records cover.

Payroll wage/salary records (also overtime, bonuses, expenses) :6 years from the end of the tax year to which they relate.

Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH) :5 years from the date on which the tests were carried out.

Records relating to children and young adults: until the child/young adult reaches the age of 21.

Retirement Benefits Schemes :6 years from the end of the scheme year in which the event took place.

Statutory Maternity Pay records including Mat B1s (also shared parental, paternity and adoption pay records) :3 years after the end of the tax year in which the maternity period ends.

Subject access request (SAR) :1 year following completion of the request.

Working time records including overtime, annual holiday, time off for dependents, etc :2 years from date on which they were made.

Recommended retention period

Record type: Statutory retention period

Actuarial valuation reports: Permanently.

Collective agreements :6 years after the agreement ends.

CCTV footage: ICO retention practice is 6 months following the outcome of any formal decision or appeal. CCTV footage may be relevant to a disciplinary matter or unfair dismissal claim

Driving offences: Must be removed once the conviction is spent under the Rehabilitation of Offenders Act 1974.

Flexible working requests :18 months following any appeal. This is because a further request cannot be made for 12 months following a request plus allowing for a 6-month tribunal limitation period on top.

Inland Revenue/HMRC approvals: Permanently.

Money purchase details: 6 years after transfer or value taken.

Parental leave: 18 years from the birth of the child

Pension records :12 years after the benefit ceases.

Pension scheme investment policies: 12 years from the ending of any benefit payable under the policy.

Personnel files and training records (including disciplinary and working time records) :6 years after employment ceases but may be unreasonable to refer to expired warnings after two years have elapsed.

Recruitment application forms and interview notes (for unsuccessful candidates) :6 months to a year. Because of the time limits in the Equality Act, relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants' documents will transfer to the personnel file.

Redundancy details, calculations of payments, refunds: 6 years from the date of redundancy.

References: Outgoing references given by an organisation should be retained for at least one year after the reference is given to meet the limitation period for potential defamation claims. However, employers may be able to justify a longer retention period of six years, if they are concerned about defending any future claims. For incoming references received from previous employers, organisations could simply retain a note that satisfactory references were received. For references of unsuccessful applicants, a retention period of nine months to a year is probably justified, because the time limit for discrimination is six months plus possible time limit extensions. Some employers

may decide they have no need to keep references for new staff once the employee has successfully completed a probationary period.

Right to work in the UK checks: Home Office recommended practice is 2 years after employment ends.

Senior executives' records (senior management team or equivalents) : Some records may need permanent retention such as documents from the company's incorporation, shareholdings, resolutions, memorandum and articles, annual returns, register of directors interests, share documents, accounts, liability policies, pension scheme documents etc most of which should be retained permanently. Retain personal records, performance appraisals, employment contracts etc for 6 years after the employee has left to reflect the main limitation period.

Statutory Sick Pay (SSP) records, calculations, certificates, self-certificates, occupational health reports. Also COVID-19-related SSP records such as the dates off sick. : Six months after the end of the period of sick leave is sensible in case of a disability discrimination claim. For personal injury claims, the limitation is 3 years. If there's a contractual claim for breach of an employment contract, then keep records for 6 years after the employment ceases. Employers should keep a record of SSP paid due to COVID-19 as HMRC may request records.

Termination of employment, for example early retirement, severance or death in service: At least 6 years although the ICO's retention schedule suggests until employee reaches age 100.

Terms and conditions including offers, written particulars, and variations: Review 6 years after employment ceases or the terms are superseded.

Timecards: 2 years after audit.

Trade union agreements: 10 years after ceasing to be effective.

Trust deeds and rules: Permanently.

Trustees' minute books: Permanently.

Works council minutes: Permanently.

Share Holders Meeting Minutes: Permanently

Your records which have reached the end of their administrative life must be destroyed in as secure a manner as is appropriate to the level of confidentiality or protective markings they bear. The methods used to destroy records must provide adequate safeguards against the accidental loss or disclosure of the contents.

A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the department responsible for the records so that the organisation is aware of those records that have been destroyed and are therefore no longer available.

What are your rights?

You have the right to confidentiality under Data Protection Law, the Human Rights Act 1998 and the Common Law Duty of Confidentiality

VERDANT

The right to be informed – you have the right to know what information we hold about you, what we use it for and if the information is shared, who it will be shared with. We do this through this privacy notice.

The right of access – to information held about you. For further information please refer to the section "How can you gain access to the information that we hold about you?"

The right to rectification – this is your right to have your personal data rectified if it is inaccurate or incomplete. If you believe that the information recorded about you is incorrect, you will need to tell us by contacting your personal representative. We will correct factual mistakes and provide you with a copy of the corrected information.

The right to erasure – this is also known as your 'right to be forgotten' where there is no compelling reason to continue processing your data in relation to the purpose for which it was originally collected or processed. Parts of your records must remain in line "Statutory record retention period". It is extremely rare that we destroy or delete records earlier than the "Recommended retention period". Email us at office@verdant-recruitment.com to send a GDPR Request

The right to restrict processing – this is your right to block or suppress the processing of your personal data. For example: if you would like to restrict processing of your information from marketing then you can do this by seeking a a request form by emailing us at office@verdant-recruitment.com

The right to data portability – this is your right to obtain and re-use any information you have provided to us as part of an automated process. At present we do not process any personal data that meets this requirement.

The right to object – this is your right to object to us processing your data. Whilst we will stop processing your data it may mean we are unable to provide a service to you. We are obligated to keep your data in line "Statutory record retention period".

Rights in relation to automated decision making and profiling – GDPR provides safeguards for individuals against the risk that a potentially damaging decision would be taken without human intervention. While we may use systems to determine how suited an individual is for a role, it does not replace decisions made by us. We use this to improve your experience when using our services.

If you have provided your consent, you have the right to withdraw your consent at any time by emailing office@verdant-recruitment.com and seeking a request to withdraw GDPR request form

You have the right to lodge a complaint with the Information Commissioner Office (ICO) if you believe that the we have not complied with the requirements of the GDPR or the DPA with regards to your personal data. Please refer to the section, "How can you contact us with queries or concerns about this privacy notice?" or "How can you make a complaint?"

How can you gain access to the information we hold about you?

Under the General Data Protection Regulations (GDPR) and Data Protection Act, you have the right to request access to the information that we hold about you using the process known as a 'Subject Access Request' (SAR).

If you would like a copy of your records, we hold you are able to submit a request by emailing office@verdant-recruitment.com

* A request for a copy is free, however we may charge an administrative fee if you require more than a single copy of your information

How can you contact us with queries or concerns about this privacy notice?

If you have any queries or concerns regarding the information that we hold about you or have a question regarding this privacy notice, then please contacts us via Email on office@verdant-recruitment.com

How can you make a complaint?

You have the right to make a complaint if you feel unhappy about how we hold, use or share your information. We would recommend that you contact us initially to talk through any concerns that you may have: Contact number is on our website www.verdant-recruitment.com

If you remain dissatisfied following the outcome of your complaint, you may then wish to contact the Information Commissioner's Office:

Web: Information Commissioner; https://ico.org.uk/

DATA CLASSIFICATION POLICY

1. Policy introduction

Here at Verdant Recruitment Ltd, we are committed to data security, the privacy of the individual and upholding all our compliance obligations under GDPR. We take our responsibilities seriously, and we recognise that the use of information assets and data form a crucial aspect of our business activity. That is why we've devised the following Data Classification Policy to outline the way in which we classify and use data.

Our Data Classification Policy is designed to ensure that:

- Verdant Recruitment Ltd adheres to all necessary legal obligations
- We implement controls to maximise return on investment
- Verdant Recruitment Ltd maintains availability, confidentiality and integrity where necessary for all data
- Our company has the ability to chart data protection levels that protect both Verdant Recruitment Ltd as well as the individuals whose personal data we must collect, process or store
- We are able to avoid threats of disclosure and/or unauthorised access to data

2. Policy values

Data classification is a vital process our company must carry out to ensure the individuals who claim a legitimate right to access information we hold are able to do so. Our data classification process must also ensure our data and any other piece of information we hold is protected from any and all individuals or organisations that should not have access to that information.

Verdant Recruitment Ltd Data Classification Policy identifies and elaborates upon the correct handling and classification processes our company must use, as per the regulatory requirements that we:

- Make data available to all those individuals who have a legitimate reason to access it
- Manage all data in line with its corresponding classification
- Maintain the integrity of all data
- Ensure all data our company holds is accurate, complete and consistent

3. Policy objectives

Verdant Recruitment Ltd Data Classification Policy has been developed to meet the following objectives:

- To outline the duties and responsibilities of Verdant Recruitment Ltd employees that ensure data is kept safe and secure
- To establish a robust data classification process that is consistent and compliant with UK regulatory requirements
- To ensure data is sufficiently protected and encrypted so that unwarranted actions will not be taken against Verdant Recruitment Ltd in the event data is lost, damaged or accessed illegally
- To avoid and minimise reputational or operational damage to Verdant Recruitment Ltd, our stakeholders, clients, customers or partners associated with compromised data

4. Policy implementation

To make sure our Data Classification Policy is effective, Verdant Recruitment Ltd will implement the following procedures:

- All users of data will be identified and provided access to data in which they have a legitimate need to access
- All data will be classified, managed and controlled in relation to its correct categorisation, as per the processes and requirements outlined within this policy
- Verdant Recruitment Ltd must ensure control mechanisms are created and implemented to protect data we collect, process or store
- All control mechanisms and classification protocols must be reviewed and amended as required by law on a regular basis
- Data users and data controllers must implement and maintain adequate levels of physical security as required, in relation to computer facilities or access terminals from which data can be viewed or accessed
- Verdant Recruitment Ltd must ensure that all data and relevant equipment is safely disposed of, as and when required

5. Obligations under GDPR (2018) and Data Protection Act 2018 (DPA)

Verdant Recruitment Ltd is committed to meet its regulatory obligations under GDPR and DPA. That is why we are committed to ensure that adequate and appropriate measures are taken to prevent the unauthorised access or illegal processing or storage of data. We are required to do everything we can, within reason, to protect the data we use and hold against destruction, accidental loss or damage.

6. Data classifications

Data that is sensitive in nature must be adequately protected at all times. To properly assign safeguards, all data that our company collects, processes or stores must be assigned one of the following classification categories:

- Public
- Open
- Confidential
- Strictly Confidential
- Secret

A vast amount of the data Verdant Recruitment Ltd uses will most likely be classed as being either 'Public' or 'Open' data. Any information relating to an individual or organisation that could identify them or is personal or private in nature must be assigned a category of either 'Confidential' or 'Strictly Confidential'.

This is to ensure Verdant Recruitment Ltd upholds its regulatory commitment to uphold the rights of individuals, as outlined under GDPR.

On rare occasions, Verdant Recruitment Ltd may wish to class data as 'Secret'. If an employee is unsure as to whether they should categorise a piece of data as being secret – or if they need assistance in classifying any other piece of data, they should consult a line manager. If no manager is available for consultation, data should default to a 'Confidential' classification.

7. Data classification types and handling procedures

To minimise discrepancies and ensure Verdant Recruitment Ltd does everything it can to uphold its regulatory commitments, the following working definitions should be associated with the aforementioned classification categories.

Public data

Public data is information or data that can be accessed by any external individual or organisation.

Types of public data might include:

- Official contact data of relevant company employees
- News updates or press releases
- Company publications
- External-facing company policies or procedures

How to handle public data:

Public data should be formatted to allow for the most basic security measures. Examples might include converting a Word document into a PDF to avoid others editing it, as this could subsequently cause some form of reputational damage.

Open

Anyone is able to access this information.

Types of open data might include:

- Official contact data e.g. full name, primary email address and telephone number
- Authorised communications, such as blogs, news articles and industry updates
- Approved company policies, guidance and processes

How to handle open data:

Open data should be formatted to allow for the most basic security measures. Examples might include converting a Word document into a PDF to avoid others editing it, as this could subsequently cause some form of reputational damage.

Confidential data

Access to confidential data must be limited only to individuals who have been granted appropriate authorisation to view or process that information.

Alternatively, there may be occasions in which unauthorised individuals or stakeholders may need to be granted access to confidential data; however, this access must only be provided on a need-to-know basis.

Types of confidential data might include:

- Someone's personal details or any information that could be used to identify them. Examples of identifiable or personal details include:
  - Name
  - Date of birth
  - Address
  - Telephone number

  - Email address
  - National Insurance number
  - Race
  - Religion
  - Health details
  - Political affiliations
  - Trade union membership
  - Criminal offences
- Employee contracts
- Non-Disclosure Agreements
- Unfinished or unapproved company documents
- Employee wage slips
- Death certificates
- PDR documentation

How to handle confidential data:

As and where required to handle confidential data, employees should exercise the following handling processes:

- Paper documents must be:
  - In secure locked storage
  - Transported in sealed envelopes only
  - Transported by an approved third-party courier service
  - Securely disposed of

- Electronic data must be:
  - Encrypted
  - Password-protected wherever possible
  - Transportation must follow secure file transfer protocol
  - Storage must be limited to secure file stores
  - Securely disposed of

Strictly confidential data

A minimal number of authorised individuals, authorities or other stakeholders may be permitted access to data that has been classified as being ‘Strictly confidential’.

Types of strictly confidential data might include:

- Bank details
- Credit card information
- Financial information
- Server information
- Usernames or passwords

- Test data
- Medical records
- Disciplinary proceedings
- Patent information
- Network information

How to handle strictly confidential data:

As and where required to handle strictly confidential data, employees should exercise the following handling processes:

- Paper documents must be:
  - In secure locked storage
  - Transported in sealed envelopes only
  - Transported by an approved third-party courier service

- Electronic data must be:
  - Encrypted
  - Password-protected wherever possible
  - Tagged
  - Transportation must follow secure file transfer protocol
  - Storage must be limited to secure file stores

Secret data

Access to data that has been classed as 'Secret' or a request to access secret data is subject to the Official Secrets Act.

Various types of secret data may require different controls and circumstances. Bearing that in mind, individual protocols should be reviewed on a case-for-case basis in line with UK Government requirements. Government advice concerning the handling of secret data should be sought.

8. Data classification markings

Data classification markings need to be clearly visible at all times and must match the classification category in which that data has been assigned. Appropriate data classification identification markings should be included either at the top, bottom or centre of each document page.

9. Reclassifying data

There may be occasions in which data must be reclassified from one data category to another

data category. The need for reclassification could depend upon a content change, or an alteration in terms of the data's intent, where it is stored or how it is being used. Before reclassifying data, a firm and justifiable rationale must be established. If in doubt, contact the Data Protection Officer or your line manager for guidance.

10. Sensitive data

It is the responsibility of the data owner or the data originator to define the category of data classification for a piece of data. Responsibility also rests with the data owner or originator to ensure that adequate protection has been afforded to that data in line with its relevant classification.

Any data that could or should be defined as being personal in nature must be afforded a higher level of protection and be treated as data that is sensitive. Personal data can be classed as information relating to an individual that could identify them. Aforementioned examples of sensitive personal data might include (among other pieces of data) a person's name, contact information, race, religion, political affiliations, sexual preference and so on.

Sensitive data must be identified and assessed on a case-for-case basis. In most cases, sensitive data will inherently be classed as confidential; thus, access and/or availability must be limited. Sensitive data which is made available in the public domain can lead to reputational damage for private individuals or company employees. As a company we must ensure that sensitive data is given sufficient protection to protect individuals, company employees and the company itself.

11. Data storage and backup

Because data is such an integral aspect of our business, it is everyone's responsibility at [COMPANY NAME] to do everything within their power to ensure that sensitive data is being collected, processed, backed up, stored and secured in line with company policy.

12. Data anonymisation

Prior to the sharing, transfer or disclosure of data, [COMPANY NAME] and its employees must take all necessary steps to ensure that the anonymity of corresponding data subjects is protected and maintained in line with our regulatory commitments.

Necessary steps may include omitting or redacting (deleting) said personal identifiers within a piece of data. Audio visual data or verbally exchanged data recordings should be likewise edited.

13. Secure data disposal

Sensitive data that is no longer needed or has reached an ‘end of life’ classification as decided upon by the relevant authorised individuals must be disposed of in a secure fashion. Examples of disposing data as stored on paper would include shredding.

14. Data security response

If data is damaged or lost, it must be immediately reported to an appropriate line manager and company Data Protection Officer, and logged as an incident requiring urgent response.

VERDANT

GDPR Terms & Conditions

These Terms and Conditions, together with any and all other documents referred to herein, set out the terms of use under which you may use this website, www.ajk-woodflooring.co.uk ("Our Site"). Please read these Terms and Conditions carefully and ensure that you understand them. Your agreement to comply with and be bound by these Terms and Conditions is deemed to occur upon your first use of Our Site. If you do not agree to comply with and be bound by these Terms and Conditions, you must stop using Our Site immediately.

1. Definitions and Interpretation

1.1 In these Terms and Conditions, unless the context otherwise requires, the following expressions have the following meanings:

- Content : means any and all text, images, audio, video, scripts, code, software, databases and any other form of information capable of being stored on a computer that appears on, or forms part of, Our Site
- System means any online communications facility that We make available on Our Site either now or in the future. This may include, but is not limited to, contact forms, email, and live chat; and
- We/us/Our means Verdant Recruitment Ltd a company registered in England and Wales under company Number : 16001061,

2. Information About Us

- 2.1 Our Site, www.verdant-recruitment.com, is owned and operated Verdant Recruitment Ltd a company registered in England and Wales under company Number : 16001061,

3. Access to Our Site

3.1 Access to Our Site is free of charge.

3.2 It is your responsibility to make any and all arrangements necessary in order to access Our Site.

3.3 Access to Our Site is provided "as is" and on an "as available" basis. We may alter, suspend or discontinue Our Site (or any part of it) at any time and without notice. We will not be liable to you in any way if Our Site (or any part of it) is unavailable at any time and for any period.

4. Intellectual Property Rights

4.1 All Content included on Our Site and the copyright and other intellectual property rights subsisting in that Content, unless specifically labelled otherwise, belongs to or has been licensed by Us. All Content is protected by applicable United Kingdom and international intellectual property laws and treaties.

4.2 Subject to sub-Clause[s] 4.3 [and 4.6] you may not reproduce, copy, distribute, sell, rent, sub-licence, store, or in any other manner re-use Content from Our Site unless given express written permission to do so by Us.

4.3 You may:

4.3.1 Access, view and use Our Site in a web browser (including any web browsing capability built into other types of software or app);

4.3.2 Download Our Site (or any part of it) for caching;

4.3.3 Print one copy of any page from Our Site;

4.3.4 Download extracts from pages on Our Site; and

4.3.5 Save pages from Our Site for later and/or offline viewing.

4.4 Our status as the owner and author of the Content on Our Site (or that of identified licensors, as appropriate) must always be acknowledged.

4.5 You may not use any Content saved or downloaded from Our Site for commercial purposes without first obtaining a licence from Us (or our licensors, as appropriate) to do so. This does not prohibit the normal access, viewing and use of Our Site for general information purposes whether by business users or consumers.

4.6 Nothing in these Terms and Conditions limits or excludes the provisions of Chapter III of the Copyrights, Designs and Patents Act 1988 'Acts Permitted in Relation to Copyright Works', covering in particular the making of temporary copies; research and private study; the making of copies for text and data analysis for non-commercial research; criticism, review, quotation and news reporting; caricature, parody or pastiche; and the incidental inclusion of copyright material.

5. Links to Our Site

5.1 You may link to Our Site provided that:

5.1.1 You do so in a fair and legal manner;

5.1.2 You do not do so in a manner that suggests any form of association, endorsement or approval on Our part where none exists;

5.1.3 You do not use any logos or trade marks displayed on Our Site without Our express written permission; and

5.1.4 You do not do so in a way that is calculated to damage Our reputation or to take unfair advantage of it.

5.1.5 You may link to any page of Our Site.

5.2 Framing or embedding of Our Site on other websites is not permitted without Our express written permission. Please contact Us for further information.

5.3 You may not link to Our Site from any other site the content of which contains material that:

5.3.1 is sexually explicit;

5.3.2 is obscene, deliberately offensive, hateful or otherwise inflammatory;

5.3.3 promotes violence;

5.3.4 promotes or assists in any form of unlawful activity;

5.3.5 discriminates against, or is in any way defamatory of, any person, group or class of persons, race, sex, religion, nationality, disability, sexual orientation, or age;

5.3.6 is intended or is otherwise likely to threaten, harass, annoy, alarm, Inconvenience, upset, or embarrass another person;

5.3.7 is calculated or is otherwise likely to deceive another person;

5.3.8 is intended or is otherwise likely to infringe (or to threaten to infringe) another person's privacy;

5.3.9 misleadingly impersonates any person or otherwise misrepresents the identity or affiliation of a particular person in a way that is calculated to deceive (obvious parodies are not included in this definition provided that they do not fall within any of the other provisions of this sub-Clause 5.4);

5.3.10 implies any form of affiliation with Us where none exists;

5.3.11 infringes, or assists in the infringement of, the intellectual property rights (including, but not limited to, copyright, trade marks and database rights) of any other party; or

5.3.12 is made in breach of any legal duty owed to a third party including, but not limited to, contractual duties and duties of confidence.

5.4 The content restrictions in sub-Clause 5.4 do not apply to content submitted to sites by other users provided that the primary purpose of the site accords with the provisions of sub-Clause 5.4. You are not, for example, prohibited from posting links on general purpose social networking sites merely because another user may post such content. You are, however, prohibited from posting links on websites which focus on or encourage the submission of such content from users.

6. Links to Other Sites

6.1 Links to other sites may be included on Our Site. Unless expressly stated, these sites are not under Our control. We neither assume nor accept responsibility or liability for the content of third party sites. The inclusion of a link to another site on Our Site is for information only and does not imply any endorsement of the sites themselves or of those in control of them.

7. Use of Our System

7.1 You may use Our System at any time to contact Us. Please note the following; you must not:

7.1.1 communicate in a way that is obscene, deliberately offensive, hateful or otherwise inflammatory;

7.1.2 submit information that promotes violence;

7.1.3 submit information that promotes or assists in any form of unlawful activity;

7.1.4 submit information that discriminates against, or is in any way defamatory of, any person, group or class of persons, race, sex, religion, nationality, disability, sexual orientation or age;

7.1.5 submit information that is intended or is otherwise likely to threaten, harass, annoy, alarm, inconvenience, upset, or embarrass another person;

7.1.6 submit information that is calculated or is otherwise likely to deceive;

7.1.7 submit information that is intended or is otherwise likely to infringe (or to threaten to infringe) another person's privacy;

7.1.8 misleadingly impersonate any person or otherwise misrepresent your identity or affiliation in a way that is calculated to deceive;

7.1.9 imply any form of affiliation with Us where none exists;

7.1.10 infringe, or assist in the infringement of, the intellectual property rights (including, but not limited to, copyright, trade marks and database rights) of any other party; or

7.1.11 submit information in breach of any legal duty owed to a third party including, but not limited to, contractual duties and duties of confidence.

7.2 We may monitor any communications made using Our System.

7.3 Any information that you send to Us through Our System may be modified by Us and, by sending us such information, you waive your moral right to be identified as the author of that information.

7.4 Any personal information sent to Us, whether through Our System or otherwise (including but not limited to your name and contact details), will be collected, used and held in accordance with your rights and Our obligations under the Data Protection Act 1998, as set out in Clause 13.

8. Disclaimers

8.1 Nothing on Our Site constitutes advice on which you should rely. It is provided for general information purposes only.

8.2 Insofar as is permitted by law, We make no representation, warranty, or guarantee that Our Site will meet your requirements, that it will not infringe the rights of third parties, that it will be compatible with all software and hardware, or that it will be secure.

8.3 We make reasonable efforts to ensure that the Content on Our Site is complete, accurate, and up-to-date. We do not, however, make any representations, warranties or guarantees (whether express or implied) that the Content is complete, accurate, or up-to-date.

8.4 No part of Our Site is intended to constitute a contractual offer capable of acceptance.

8.5 We make reasonable efforts to ensure that any and all pricing information shown on Our Site is correct at the time of going online. We reserve the right to change prices at any time and may add or remove special offers and promotions from time to time.

8.6 Whilst every reasonable effort has been made to ensure that all representations and descriptions of goods and services available from Us correspond to the actual goods and services available, minor variations or errors may occur. In the event of any discrepancy, please contact us.

9. Our Liability

9.1 To the fullest extent permissible by law, We accept no liability to any user for any loss or damage, whether foreseeable or otherwise, in contract, tort (including negligence),for breach of statutory duty, or otherwise, arising out of or in connection with the use of (or inability to use) Our Site or the use of or reliance upon any Content included on Our Site.

9.2 To the fullest extent permissible by law, We exclude all representations, warranties, and guarantees (whether express or implied) that may apply to Our Site or any Content included on Our Site.

9.3 If you are a business user, We accept no liability for loss of profits, sales, business or revenue; loss of business opportunity, goodwill or reputation; loss of anticipated savings; business interruption; or for any indirect or consequential loss or damage.

9.4 We exercise all reasonable skill and care to ensure that Our Site is free from viruses and other malware. We accept no liability for any loss or damage resulting from a virus or other malware, a distributed denial of service attack, or other harmful material or event that may adversely affect your hardware, software, data or other material that occurs as a result of your use of Our Site (including the downloading of any Content from it) or any other site referred to on Our Site.

9.5 We neither assume nor accept responsibility or liability arising out of any disruption or non-availability of Our Site resulting from external causes including, but not limited to, ISP equipment failure, host equipment failure, communications network failure, natural events, acts of war, or legal restrictions and censorship.

9.6 Nothing in these Terms and Conditions excludes or restricts Our liability for fraud or fraudulent misrepresentation, for death or personal injury resulting from negligence, or for any other forms of liability which cannot be excluded or restricted by law. For full details of consumers' legal rights, including those relating to digital content, please contact your local Citizens' Advice Bureau or Trading Standards Office.

10. Viruses, Malware and Security

10.1 We exercise all reasonable skill and care to ensure that Our Site is secure and free from viruses and other malware.

10.2 You are responsible for protecting your hardware, software, data and other material from viruses, malware, and other internet security risks.

10.3 You must not deliberately introduce viruses or other malware, or any other material which is malicious or technologically harmful either to or via Our Site.

10.4 You must not attempt to gain unauthorised access to any part of Our Site, the server on which Our Site is stored, or any other server, computer, or database connected to Our Site.

10.5 You must not attack Our Site by means of a denial of service attack, a distributed denial of service attack, or by any other means.

10.6 By breaching the provisions of sub-Clauses 10.3 to 10.5 you may be committing a criminal offence under the Computer Misuse Act 1990. Any and all such breaches will be reported to the relevant law enforcement authorities and We will cooperate fully with those authorities by disclosing your identity to them. Your right to use Our Site will cease immediately in the event of such a breach.

11. Acceptable Use Policy

11.1 You may only use Our Site in a manner that is lawful. Specifically:

11.1.1 you must ensure that you comply fully with any and all local, national or international laws and/or regulations;

11.1.2 you must not use Our Site in any way, or for any purpose, that is unlawful or fraudulent;

11.1.3 you must not use Our Site to knowingly send, upload, or in any other way transmit data that contains any form of virus or other malware, or any other code designed to adversely affect computer hardware, software, or data of any kind; and

11.1.4 you must not use Our Site in any way, or for any purpose, that is intended to harm any person or persons in any way.

11.2 We reserve the right to suspend or terminate your access to Our Site if you materially breach the provisions of this Clause 11 or any of the other provisions of these Terms and Conditions. Specifically, We may take one or more of the following actions:

11.2.1 suspend, whether temporarily or permanently, your right to access Our Site;

11.2.2 issue you with a written warning;

11.2.3 take legal proceedings against you for reimbursement of any and all relevant costs on an indemnity basis resulting from your breach;

11.2.4 take further legal action against you as appropriate;

11.2.5 disclose such information to law enforcement authorities as required or as We deem reasonably necessary; and/or

11.2.6 any other actions which We deem reasonably appropriate (and lawful).

11.3 We hereby exclude any and all liability arising out of any actions (including, but not limited to those set out above) that We may take in response to breaches of these Terms and Conditions.

12. Privacy and Cookies

12.1 Use of Our Site is also governed by Our Cookie and Privacy Policies. Please contact us if you wish to see a copy of these policies. These policies are incorporated into these Terms and Conditions by this reference.

13. Data Protection

13.1 All personal information that We may collect (including, but not limited to, your name and contact details) will be collected, used and held in accordance with the provisions of the Data Protection Act 1998 and your rights and Our obligations under that Act.

13.2 We may use your personal information to:

13.2.1 Reply to any communications you send to Us;

13.2.2 [Send you important notices, as detailed in Clause 14;]

13.3 We will not pass on your personal information to any third parties [without first obtaining your express permission to do so].

14. Communications from Us

14.1 If We have your contact details, we may from time to time send you important notices by email. Such notices may relate to matters including, but not limited to, service changes and changes to these Terms and Conditions.

14.2 We will never send you marketing emails of any kind without your express consent. If you do give such consent, you may opt out at any time. Any and all marketing emails sent by Us include an unsubscribe link. If you opt out of receiving emails from Us at any time, it may take up to 20 business days to take effect.

14.3 For questions or complaints about communications from Us (including, but not limited to marketing emails), please contact Us at office@verdant-recruitment.com

15. Changes to these Terms and Conditions

15.1 We may alter these Terms and Conditions at any time. Any such changes will become binding on you upon your first use of Our Site after the changes have been implemented. You are therefore advised to check this page from time to time.

15.2 In the event of any conflict between the current version of these Terms and Conditions and any previous version(s), the provisions current and in effect shall prevail unless it is expressly stated otherwise.

16. Contacting Us

16,1 To contact Us, please use contact form within contact page of our website or alternatively email us at office@verdant-recruitment.com,

17. Law and Jurisdiction

17.1 These Terms and Conditions, and the relationship between you and Us (whether contractual or otherwise) shall be governed by, and construed in accordance with the law of [England & Wales] [Northern Ireland] [Scotland].

17.2 If you are a consumer, you will benefit from any mandatory provisions of the law in your country of residence. Nothing in Sub-Clause 17.1 above takes away or reduces your rights as a consumer to rely on those provisions.

17.3 If you are a consumer, any dispute, controversy, proceedings or claim between you and Us relating to these Terms and Conditions, or the relationship between you and Us (whether contractual or otherwise) shall be subject to the jurisdiction of the courts of England, Wales, Scotland, or Northern Ireland, as determined by your residency.

17.4 If you are a business, any disputes concerning these Terms and Conditions, the relationship between you and Us, or any matters arising therefrom or associated therewith (whether contractual or otherwise) shall be subject to the [non] exclusive jurisdiction of the courts of England & Wales.

This Policy has been approved and authorised by the directors of Verdant Recruitment Ltd

October 2024

VERDANT

GENERAL DATA PROTECTION NOTICE

Verdant Recruitment Ltd Data Protection Notice

Verdant Recruitment Ltd collects, processes and stores the information and personal data you submit to our website in relation to reviewing suitability to review for roles Verdant Recruitment Ltd are looking to fill for its client. All processing activities shall be carried out in accordance with your individual rights as defined by the European Union's General Data Protection Regulation.

Please note that by submitting information about yourself through our website, you are agreeing for Verdant Recruitment Ltd to process and store that data. This data shall be stored only for the duration of the previously outlined purpose for collection. We never store or process your data longer than we need to, and we do not use your data for any purpose other than those you have agreed to.

The data you submit to our website will never be shared with or transferred to a third-party organisation. The following partners are exempt from this policy as they assist Verdant Recruitment Ltd in processing your personal data and delivering its services, Job Search Engines/Organisations, Social media Organisations.

You reserve the right to request Verdant Recruitment Ltd update your personal data at any time. You can also request information about your personal data, withdraw your consent for us to process your information or request a transfer or deletion of your data.

For more information about Verdant Recruitment Ltd and how we protect and secure your data, consult our Privacy Policy found on our website.

VERDANT

HEALTH & SAFETY AT WORK POLICY STATEMENT

The Directors of Verdant Recruitment Ltd recognise that the health, safety and welfare of our employees, is of paramount importance. We aim to provide and maintain an appropriate place of work, maintain suitable equipment and ensure safe systems of work for all our employees.

We also accept our responsibility for the health and safety of other persons who may be affected by our activities.

We shall strive to ensure continual improvement within our safety management system, whilst recognising the requirement to meet our legal obligations.

We shall ensure a systematic approach to the assessment of risk is undertaken and that the preventative and protective measures identified as an outcome of these risk assessments are implemented.

We recognise the importance of employee participation, and we shall ensure direct consultation with our employees on all matters regarding health and safety. We shall ensure that our employees are provided with information, instruction and training, and that they are technically competent for the roles they undertake.

Whilst our employees can expect to have an appropriate place of work in which risks are managed to an acceptable level, employees also have roles and responsibilities in delivering an appropriate level of health and safety performance across the business.

VERDANT

Modern Slavery Policy

Modern Slavery is an abhorrent and heinous violation of fundamental human rights. The offences of 'slavery', servitude, forced or compulsory labor' and 'human trafficking is a criminal offence under The Modern Slavery Act 2015.

Verdant Recruitment Limited fully support the eradication of this crime and have a zero tolerance policy towards Modern Slavery and Human Trafficking and the exploitation of others for personal or commercial gain.

We are committed to acting ethically and with integrity in all our business dealings and relationships and to implementing and enforcing effective systems and controls to ensure modern slavery is not taking place anywhere in our own business or in any of our supply chains.

Verdant Recruitment Ltd will:

- Monitor suppliers and subcontractors both in the UK and in the country of origin of manufacture with the aim of checking that fair wages are paid and that working conditions are acceptable and that employees are free to leave their employment.
- Check that all personnel working on our sites are entitled to work in the UK by reviewing original passports, visa, taxation and other relevant documentation.
- Monitor that all personal working on our sites are paid appropriately and at least the minimum wage set by the government, and are free to leave their employment.
- Provide training on this policy to all our employees.
- Communicate our Modern Slavery Policy to all our subcontractors, joint venture partners, consultants, and other agents, third party representatives and business partners at the outset of our business relationship and appropriately thereafter.
- Introduce a contractual provision for all suppliers to confirm their adherence to this policy and accept our right to audit their activities and (where practicable) relationships, both routinely and at times of reasonable suspicion.
- Encourage the reporting of concerns and safeguard individuals in accordance with our Whistleblowing Policy
- The policy is in compliance with Section 54 of The Modern Slavery Act 2015 and will be reviewed and updated annually.

VERDANT

Quality Policy for Verdant Recruitment Ltd

Purpose:

At Verdant Recruitment Ltd, we are committed to providing exceptional recruitment services that meet the needs of our clients and candidates. Our goal is to ensure a seamless and effective recruitment process that fosters lasting relationships and supports the growth of businesses and individuals alike.

Policy Statement:

Verdant Recruitment Ltd strives to uphold the highest standards of quality in all our recruitment activities. We aim to deliver services that exceed client and candidate expectations through:

1. Client-Centric Approach:
   We prioritize understanding our clients' unique requirements and culture to deliver tailored recruitment solutions that align with their goals.
2. Candidate Experience:
   We are dedicated to providing a positive and transparent experience for all candidates, ensuring timely communication, support, and feedback throughout the recruitment process.
3. Continuous Improvement:
   We actively seek feedback from clients and candidates to enhance our processes, services, and outcomes. Regular training and development for our team are essential to maintaining high standards.
4. Compliance and Integrity:
   We adhere to all relevant legislation and best practices in recruitment. Our ethical approach ensures fairness, diversity, and inclusivity in our hiring processes.
5. Performance Measurement:
   We establish measurable goals and regularly assess our performance against them. This includes tracking client satisfaction, candidate success rates, and overall service quality.

Commitment:

The management and staff of Verdant Recruitment Ltd are committed to fostering a culture of quality throughout our organization. We will provide the necessary resources and training to ensure that every team member understands their role in delivering quality service.

Review:

This policy will be reviewed annually to ensure its effectiveness and relevance. We welcome feedback from all Clients ,Candidates and Staff to help us continually improve our quality standards.

Effective Date:

October 2024

VERDANT

Carbon Reduction Plan for Verdant Recruitment Ltd

1. Introduction

- **Company Overview:** Briefly describe Verdant Recruitment Ltd, its mission, and its commitment to sustainability.
- **Purpose of the Plan:** Outline the goal of reducing carbon emissions and promoting environmental responsibility.

2. Current Carbon Footprint Assessment

- **Data Collection:** Gather data on current energy usage, travel, waste management, and office resources.
- **Baseline Emissions:** Calculate the carbon footprint using a recognized methodology (e.g., Greenhouse Gas Protocol).

3. Reduction Goals

- **Short-term (1-2 years):** Aim for a 10% reduction in carbon emissions.
- **Medium-term (3-5 years):** Target a 25% reduction.
- **Long-term (5+ years):** Strive for net-zero emissions by a specific year.

4. Strategies for Reduction

- **Energy Efficiency:**
  - Transition to energy-efficient lighting and appliances.
  - Implement smart energy management systems.
- **Remote Work Policies:**
  - Encourage remote work to reduce commuting emissions.
  - Provide support for home office setups that use energy-efficient equipment.
- **Sustainable Travel:**
  - Promote the use of public transportation, cycling, or walking for client meetings.
  - Offer incentives for employees to use electric or hybrid vehicles.
- **Waste Management:**
  - Implement recycling programs and reduce single-use plastics.
  - Encourage digital document management to minimize paper use.
- **Sustainable Procurement:**
  - Source office supplies from eco-friendly vendors.
  - Evaluate suppliers based on their sustainability practices.

5. Employee Engagement and Training

- **Awareness Programs:** Conduct workshops on sustainability practices.
- **Green Champions:** Appoint team members to lead sustainability initiatives.
- **Feedback Mechanisms:** Encourage suggestions from employees on improving sustainability efforts.

VERDANT

6. Monitoring and Reporting

- **Regular Assessments:** Conduct annual carbon footprint assessments to track progress.
- **Reporting:** Share results and progress with employees and stakeholders.

7. Partnerships and Certifications

- **Collaboration:** Partner with local environmental organizations to support sustainability initiatives.
- **Certifications:** Consider obtaining sustainability certifications (e.g., ISO 14001) to enhance credibility.

8. Conclusion

- Reiterate the commitment to reducing carbon emissions and the importance of collective effort in achieving sustainability goals.

Next Steps

- Establish a timeline for implementing each strategy.
- Assign responsibilities to team members for monitoring progress and reporting.