Privacy Policy

Aim of the policy

Nevalee Business Solutions is a responsible and ethical employer. We regard the lawful, transparent and fair treatment of personal data as very important to maintaining confidence. We collect personal data only for specified, explicit and legitimate purposes and keep it for a specified period. Accuracy is very important, and we take all reasonable steps to ensure inaccurate personal data is rectified or deleted without delay. We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

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.

Whom this privacy notice is addressed to

This privacy notice is addressed the organisation's employees, workers, contractors, volunteers, interns, apprentices, and former employees, referred to as HR-related personal data.

It does not apply to the personal data of job applicants, client, customers, suppliers or other personal data processed for business purposes, for which we have a separate privacy notice.

Data protection principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection (employment) policy.

Who does what: the legal bits

We hold and use your personal information in accordance with the Data Protection Act 1998 and in accordance with the requirements of the UK's equivalent of the General Data Protection Regulation (GDPR).

Data controller: Nevalee Business Solutions (registered in England No. 08064917), is a 'data controller' and gathers and uses certain information about you.

Nominated representative: if you have any enquiries about your data or how the organisation controls and processes it, please get in touch with the Managing Director Keith Thompson

Personal data: is any information that relates to an individual who can be identified from that information
Processing: is any use that is made of data, including collecting, storing, amending, disclosing or destroying it

Special categories of personal data mean information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data

Criminal records data: means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings

About the information we collect and hold

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

1. How we collect your data.

1.1 All personal information, such as your name, postal and e-mail address, or telephone number, is considered private and confidential. This personal information is stored in a secure location, is accessible only by designated staff, and is used only for the purposes that you have given us permission for e.g., provision of services.

1.2 Information we get from third parties: The majority of information we collect, we collect directly from you. However, we might collect personal data about you from other sources, such as publicly available materials such as social media, LinkedIn or trusted third parties.

1.3 The Company guarantees that the data is only accessible by designated staff.

2. How we use your data

We use your personal data to operate our business and provide you with any services you've requested, and to manage our relationship with you. We may also use your personal data for other purposes, which may include the following:

2.1 To provide you with information you've requested from us (like training or education materials) or information we are required to send to you

2.2 To inform you of operational communications, like changes to our websites and services, security updates, or assistance with using our websites and services

2.3 To undertake marketing communications about a product or service offered directly by Nevalee Business Solutions we think you might be interested in.

2.4 To ask you for feedback or to take part in any research we are conducting (which we may engage a third party to assist with).

2.5 To support you: This may include assisting with the resolution of technical support issues or other issues relating to the websites or services, whether by email, in-app support or otherwise.

2.6 To enhance our websites and services and develop new ones: For example, by tracking and monitoring your use of our websites and services so we can keep improving, or by carrying out technical analysis of our websites and services so that we can optimise your user experience and provide you with more efficient tools.

2.7 To detect and prevent any fraudulent or malicious activity, and make sure that everyone is using our websites and services fairly and in accordance with the contractual agreements.

3. How do we Protect it?

The company is committed to protecting the security of your personal information and we take all reasonable precautions to protect it from unauthorised access, modification or disclosure.

Your personal information is stored on secure servers that have antivirus \ anti malware software and use SSL Certificates issued by leading certificate authorities so that all data transferred between you and the Service is encrypted.

However, the Internet is not in itself a secure environment, and we cannot give an absolute assurance that your information will be secure at all times. Transmission of personal information over the Internet is at your own risk and you should only enter, or instruct the entering of, personal information to the service within a secure environment.

We will advise you at the first reasonable opportunity upon discovering or being advised of a security breach where your personal information is lost, stolen, accessed, used, disclosed, copied, modified, or disposed of by any unauthorised persons or in any unauthorised manner.

4. How long do we keep it?

The length of time we keep your personal data depends on what it is and whether we have an ongoing business need to retain it (for example, to provide you with a service you've requested or to comply with applicable legal, tax or accounting requirements).

We'll retain your personal data for as long as we have a relationship with you and for a period of time afterwards where we have an ongoing business need to retain it, in accordance with our data retention policies and practices. Following that period, we'll make sure it's deleted or anonymised. For more information, please request a copy of the Data Retention Policy.

5. Do we share your data?

We never sell or share your personal information with other organisations to use for their own purposes.

We at times require to share your data with third parties who provide a service to us and are our data processors. We employ other companies and individuals to perform functions on our behalf. Examples include web hosting, accountancy, HR, providing marketing assistance, processing payments. These data processors have access to personal information needed to perform their functions but may not use it for other purposes. We require these third parties to comply strictly with our instructions and data protection laws and will make sure that appropriate controls are in place.

Where we are under a duty to disclose your personal information to comply with any legal obligation (for example to government bodies and law enforcement agencies), or to enforce or apply our rights (including in relation to our website or other applicable terms and conditions) or to protect ourselves (for example, in cases of suspected fraud or defamation).

6. Can you request access to your personal information?

You may request access to the information we hold about you, known as a Data Subject Access Request DSAR, or request that we update or correct any personal information we hold about you, by setting out your request in writing and sending it to us at DataProtection@nevaleebusinesssolutions.co.uk

The company will process your request as soon as reasonably practicable, provided we are not otherwise prevented from doing so on legal grounds. If we are unable to meet your request, we will let you know why. For example, it may be necessary for us to deny your request if it would have an unreasonable impact on the privacy or affairs of other individuals, or if it is not reasonable and practicable for us to process your request in the manner you have requested. In some circumstances, it may be necessary for us to seek to arrange access to your personal information through a mutually agreed intermediary.

If your DSAR is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond and will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether we will respond to it.

Other rights
You have several other rights in relation to your personal data. You can require us to:

- Rectify inaccurate data
- Stop processing or erase data that is no longer necessary for the purposes of processing
- Stop processing or erase data if your interests override our legitimate grounds for processing data (where we rely on our legitimate interests as a reason for processing data)
- Stop processing or erase data if processing is unlawful
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override our legitimate grounds for processing data

To ask us to take any of these steps, you should send the request to our Nominated Representative Keith Thompson,

7. Nevalee Business Solutions has a privacy complaints process

If you're not happy with how we are processing your personal data, please let us know by sending an email to DataProtection@nevaleebusinesssolutions.co.uk. We will review and investigate your complaint and try to get back to you within a reasonable time frame. You can also complain to your local data protection authority. They will be able to advise you how to submit a complaint.

8. Individual responsibilities

You too have a responsibility for helping us keep your personal data up to date. You must let us know if data provided to us changes, for example if you move house or change your bank details.

You can do this by informing Stella Thompson who will be happy to help you.

You may have access to the personal data of other employees, of our customers and clients during your employment, contract, volunteer period, or apprenticeship with us. Where this is the case, we rely on you to help meet our data protection obligations to employees, customers and clients.

If you have access to personal data, you must:

- not access data unless you have authority to access it and then only for authorised purposes
- not disclose data except to individuals and entities (whether inside or outside the organisation) who have appropriate authorisation
- keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction)
- not remove personal data, or devices containing or that can be used to access personal data, from our premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- not store personal data on local drives or on personal devices that are used for work purposes

If you do not observe these requirements, it may amount to a disciplinary offence to be dealt with under our disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice

9. This policy may be updated from time to time

The company reserves the right to change this Policy at any time, and any amended Policy is effective upon posting to the Website. The company will make every effort to communicate any significant changes to you via email. Your continued use of the Service will be deemed acceptance of any amended Policy.

This procedure has been approved & authorised by:

Name: Mr. K G Thompson

Position: Managing Director

Date: September 2021

Signature: