UK GDPR PRIVACY NOTICE

What is the purpose of this document?

Barbourne Brook Limited is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR). It applies to all employees, workers and contractors.

This notice applies to current and former employees, workers and contractors. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using that information and what your rights are under the data protection legislation. Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the person's identity has been removed (anonymous data). There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health, sexual orientation or criminal convictions. Breach of the data protection legislation, including the UK GDPR rules can cause distress to the individuals affected by the breach and is likely to leave the Company at risk of serious financial consequences.

If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the Company's Data Representative, Maria Jenkins (maria@barbournebrook.co.uk).

This policy does not form part of a contract of employment. However, it is mandatory that all employees, workers or contractors must read, understand and comply with the content of this policy and you must attend associated training relating to its content and operation. Failure to adhere to this policy is likely to be regarded as a serious disciplinary matter and will be dealt with under the Company's disciplinary rules and procedures.

The kind of information we hold about you?

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the person's identity has been removed (anonymous data). There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health, sexual orientation or criminal convictions.
We will collect, store and use the following categories of personal information about you:
Personal contact details such as name, title, addresses, telephone numbers and personal email addresses.

- Date of birth.
- Gender.
- Marital status.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.

• Leaving date and your reason for leaving.
• Location of employment or workplace.
• Copy of driving licence.
• Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
• Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
• Compensation history.
• Performance information.
• Disciplinary and grievance information.
• Photographs.
We may also collect, store and use the following more sensitive types of personal information:
• details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
• any health information in relation to a claim made under the permanent health insurance scheme; and
• where you leave employment and the reason for leaving is related to your health, information about that condition is needed for pensions and permanent health insurance purposes.

What are the UK GDPR principles?

We are a data "controller". This means that we are required by law to ensure that everyone who processes personal data and special categories of personal data during the course of their work with us does so in accordance with the data protection legislation, including the UK GDPR principles. We are required under data protection legislation to notify you of the information contained in this privacy notice.
• We will comply with data protection law, which says that the personal information we hold about you must be: Personal data must be processed in a lawful, fair and transparent way.
• The purpose for which the personal information is collected must be specific, explicit and legitimate.
• The collected personal data must be adequate and relevant to meet the identified purpose.
• The information must be accurate and kept up to date.
• The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
• The personal data must be kept confidential and secure and only processed by authorised personnel.

How is your personal information collected?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers.
We will collect additional personal information during your employment with us, including job-related activities.

Other rules under the UK GDPR state that:

• The transfer of personal data to a country or organisation outside the UK should only take place if appropriate safeguarding measures are in place to protect the security of that data.
• The data subject must be permitted to exercise their rights in relation to their personal data.

The Company and all employees must comply with these principles and rules at all times in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.
You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

How we will use information about you?

Whilst carrying out your work activities you are likely to process personal data. The Company will only expect you to process personal data where the business has a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

- Consent has been obtained from the data subject to process their personal data for specified purposes.
- Where we need to perform the contract we have entered into with the data subject, either for employment or commercial purposes.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

There are other rare occasions where you may need to process the data subject's personal information. These include:

- Where we need to protect the data subject's interests (or someone else's interests).
- Where it is needed in the public interest IF RELEVANT or for official purposes.

You must always ensure that you keep a documentary inventory of the legal basis (or bases) which is being relied on in respect of each processing activity which you perform.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment using CV application.
- Determining the terms on which you work for us.
- Determining whether your engagement is deemed employment for the purposes of Chapter 10 of Part 2 of the Income Tax (Earnings and Pensions) Act 2003 (ITEPA 2003) and providing you with a status determination statement in accordance with the applicable provisions of ITEPA 2003.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Providing the following benefits to you:
- Healthcare Salary Sacrifice Scheme
- Inviting you to participate in any share plans operated by us or any group company.
- Granting awards under any share plans operated by us.
- Administering your participation in any share plans operated by us or any group company, including communicating with you about your participation and collecting any tax and NICs due on any share awards.
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Liaising with the trustees or managers of a pension arrangement operated by us or any group company, your pension provider and any other provider of employee benefits.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.

• Complying with health and safety obligations.
• To prevent fraud.
• To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
• To conduct data analytics studies to review and better understand employee retention and attrition rates.
Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.
Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

Special categories of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:
1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme].
4. Where it is necessary to protect you or another person from harm.
Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Situations in which we will use your sensitive personal information

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive personal information are listed below.
• We will use information about your physical or mental health, or disability status, to: • ensure your health and safety in the workplace;
• assess your fitness to work;
• provide appropriate workplace adjustments;
• monitor and manage sickness absence; and
• administer benefits including statutory maternity pay, statutory sick pay[,][and] pensions [and permanent health insurance.
We need to process this information to exercise rights and perform obligations in connection with your employment.
• If you leave employment and under any share plan operated by us or any group company the reason for leaving is determined to be ill health, injury or disability, we will use information about your physical or mental health, or disability status, in reaching a decision about your entitlements under the share plan.

• If you apply for an ill-health pension under a pension arrangement operated by us or any group company, we will use information about your physical or mental health in reaching a decision about your entitlement.

• If we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental or emotional harm or to protect physical, mental or emotional well-being.

If you are unsure about how you should process general personal data or special categories of personal data, you must contact Maria Jenkins.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.
We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This is usually where that processing is necessary to carry out our obligations and provided we do so in line with our Data Protection Policy.
We do not envisage that we will hold information about criminal convictions.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:
1. Where we have notified you of the decision and given you one month to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.
If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.
You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.
We do not envisage that any decisions will be taken about you using automated means. However, we will notify you in writing if this position changes.

Kept for longer than is necessary

The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
To determine the appropriate retention period for personal data, we consider:
• The amount, nature and sensitivity of the personal data.
• The potential risk of harm from unauthorised use or disclosure of your personal data.

• The purposes for which we process your personal data and whether we can achieve those purposes through other means.
• The applicable legal requirements.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use that information without further notice to you. Once you are no longer an employee, worker or contractor of the company, we will retain and securely destroy your personal information in accordance with [our Data Retention Policy OR applicable laws and regulations].

Kept confidential and secure

The personal data must be kept confidential and secure and only processed by authorised personnel.
To achieve this you must follow these steps:
• The Company has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. These procedures must always be adhered to and not overridden or ignored.
• Where the Company provides you with code words or passwords to be used before releasing personal information, for example by telephone, you must strictly follow the Company's requirements in this regard.
• Only transmit personal information between locations by e-mail if a secure network is in place, for example, encryption is used for e-mail.
• Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
• Do not access another employee's records without authority as this will be treated as gross misconduct and it is also a criminal offence.
• Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
• Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager.
• Ensure that when working on personal information as part of your job duties when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security.
• Ensure that hard copy personal information is disposed of securely, for example cross-shredded.
• Manual personnel files and data subject files are confidential and are stored online in a secure location. Only authorised employees have access to these files. For a list of authorised employees, please contact Maria Jenkins.
• No data is stored on memory sticks, discs, portable hard drives or other removable storage media.
• Data held on computers are stored confidentially by means of encryption and password protection.
• The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed. More information on the Company's security policies can be obtained from Maria Jenkins.

Transfer to another country

Transfer of personal data to countries or organisations outside of the UK should only take place if appropriate safeguarding measures are in place to protect the security of that data.
We do not generally have a need to transfer data outside of the UK. However, if you are requested to transfer personal data to a country or organisation outside of the UK you must not transfer personal data to a country or organisation unless you have in place safeguards to ensure this is done in a legally compliant manner. You must speak to Maria Jenkins before you send personal data outside of the UK.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available from your Maria Jenkins.
Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.
We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Additionally, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.
We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Right of access, correction, erasure and restriction

The data subject must be permitted to exercise their rights in relation to their personal data.

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.
Under the UK GDPR, subject to certain legal limitations, data subjects have available a number of legal rights regarding how their personal data is processed. At any time a data subject can request that the Company should take any of the following actions, subject to certain legal limitations, with regard to their personal data:
• Allow access to the personal data. 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 corrections to be made to data. This enables you to have any incomplete or inaccurate information we hold about you corrected.
• Request erasure of data. 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 the processing of data 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 that processing restrictions be put in place. 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 a transfer of personal data

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 [DPO OR data privacy manager] in writing.

How should you respond to a data subject request?

You must follow the Company's data subject access procedure which details how to deal with requests and it describes the circumstances where a fee may be charged. The procedure includes the following:

• Always verify the identity of the person making a data subject request and the legitimacy of the request.
• If you are unsure as to whether you are authorised to action the request check the privacy notice to ascertain who is authorised to deal with data subject requests. If you are still unsure how to handle the enquiry, you should forward this to Maria Jenkins.
• If you are authorised to deal with the request do not give out confidential personal information unless you have received the appropriate consent from the data subject. Seek explicit written consent to process the data subject request and ensure that you keep a clear audit trail of the request and your response.
• Do not share personal information with a third party, unless the data subject has given their explicit prior consent to the sharing of their information. A third party is anyone who is not the actual data subject and can include a family member of the data subject.
• Take great care not to accidentally share information with an unauthorised third party.

Be aware that those seeking information sometimes use deception in order to gain access to it.

Exemptions

In limited circumstances there are certain categories of personal data which are exempt from the UK GDPR regime. In an employment context these include:
• Confidential references that are given by the Company to third parties or received by the Company from third parties. Only designated line managers can give Company references. Confidential references will not be provided unless the Company is sure this is the employee's wish.
• Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
• Data which is required by law to be publicly available.
• Documents subject to legal professional privilege.

Action to be taken in the event of a data protection breach

A personal data breach will arise whenever: 1) any personal data is lost, destroyed, corrupted or disclosed; 2) if someone accesses the data or passes it on without proper authorisation; or 3) if the data is made unavailable and this unavailability has a significant negative effect on a data subject.
In the event of a security incident or breach, do not try to handle this yourself.
You must follow the Company's Data Breach Policy which includes immediately informing Maria Jenkins so that steps can be taken to:
• Contain the breach;
• Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
• To limit the scope of the breach by taking steps to mitigate the effects of the breach.

Maria Jenkins will determine within 72 hours the seriousness of the breach and if the Information Commissioner's Office (ICO) and/or data subjects need to be notified of the breach.

Record keeping

As we have fewer than 250 employees, we only need to document processing activities that:
• are not occasional; or
• could result in a risk to the rights and freedoms of individuals; or
• involve the processing of special categories of data or criminal conviction and offence data.

Training

All employees that handle personal information of individuals must have a basic understanding of the data protection legislation, including the UK GDPR. Staff with duties such as computer and internet security, marketing and database management may need specialist training to make them aware of particular data protection requirements in their work area.

We will provide you with continuous training and updates on how to process personal data in a secure and confidential manner and in accordance with the spirit of the data protection legislation, including the UK GDPR. You will be required to attend all training and to keep yourself informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.
You must regularly review all your data processing activities and ensure that you are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

Sharing personal data

We may have to share your data with third parties, including third-party service providers and other entities in the group. We require third parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside the UK. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

Third parties includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, and IT services.
We will share personal data regarding your participation in any pension arrangement operated by us or any group company with the scheme managers of the arrangement in connection with the administration of the arrangements.
How secure is my information with third-party service providers and other entities in our group?
All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.
When might you share my personal information with other entities in the group?
We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.
We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC.

Direct Marketing

We are subject to specific rules under the UK GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing and we must ensure that data subjects are given this option at first point of

contact. When a data subject exercises their right to reject marketing you must desist immediately from sending further communications.

Complaints

We have appointed Maria Jenkins to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information please contact Maria Jenkins. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO) with respect to data protection issues.

Changes to this policy

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact Maria Jenkins.

If you have any questions about this privacy notice, please contact Maria Jenkins.

Signed: 
Print Name: MARIA JENKINS