



Data Protection Policy

1 Introduction and scope

- 1.1 The Company obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former staff for a number of specific lawful purposes as set out in the Company's data protection privacy notices.
- 1.2 For the purposes of this policy, staff include: employees, workers, consultants, contractors, volunteers and apprentices.
- 1.3 This policy is non-contractual and the Company may amend it at any time. The Company will also review, and if necessary update, this policy in accordance with our data protection obligations.
- 1.4 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.
- 1.5 Our Data Protection Contact is Alison Bond, Director, who can be contacted on 07730 308691 or at alison@whbond.co.uk.

2 Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using

or doing anything with it;

pseudonymised means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

sensitive personal information (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

3 Data protection principles

3.1 The Company will comply with the following data protection principles when processing personal information:

3.1.1 we will process personal information lawfully, fairly and in a transparent manner;

3.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

3.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

3.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

3.1.5 we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

3.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

4 Basis for processing personal information

4.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

4.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take

steps at the request of the data subject prior to entering into a contract;

- (c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;
- (d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
- (e) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

4.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

4.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

4.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

4.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 5.1.2 below), and document it; and

4.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5 Sensitive personal information

5.1 The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

5.1.1 we have a lawful basis for doing so as set out in paragraph 4.1.1 above; and

5.1.2 one of the special conditions for processing sensitive personal information applies, e.g.:

- (a) the data subject has given explicit consent;
- (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;
- (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
- (d) processing relates to personal data which are manifestly made public by the data subject;
- (e) the processing is necessary for the establishment, exercise or defence of legal claims; or

- (f) the processing is necessary for reasons of substantial public interest.

- 5.2 Before processing any sensitive personal information, staff must notify our Data Protection Contact of the proposed processing so that they may assess whether the processing complies with the criteria noted above.
- 5.3 Sensitive personal information will not be processed until the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
- 5.4 The Company will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

6 Criminal records information

Criminal records information will only be sought at recruitment as set out in our privacy notice.

7 Data protection impact assessments (DPIAs)

- 7.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:
 - 7.1.1 whether the processing is necessary and proportionate in relation to its purpose;
 - 7.1.2 the risks to individuals; and
 - 7.1.3 what measures can be put in place to address those risks and protect personal information.
- 7.2 During the course of any DPIA, the employer will, where appropriate, seek the views of employees (this may be a representative group) and any other relevant stakeholders.

8 Documentation and records

- 8.1 We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information.
- 8.2 As part of our record of processing activities we document, or link to documentation, on:
 - 8.2.1 information required for privacy notices;
 - 8.2.2 records of consent;
 - 8.2.3 controller-processor contracts;
 - 8.2.4 the location of personal information;
 - 8.2.5 DPIAs; and
 - 8.2.6 records of data breaches.
- 8.3 We may document our processing activities in electronic form so we can add, remove and amend information easily.

9 Individual rights

- 9.1 You (in common with other data subjects) have the following rights in relation to your personal information:
- 9.1.1 to be informed about how, why and on what basis that information is processed—see the Company's data protection privacy notice;
 - 9.1.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see section Subject access requests below;
 - 9.1.3 to have data corrected if it is inaccurate or incomplete;
 - 9.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
 - 9.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and
 - 9.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).
- 9.2 If you wish to exercise any of the rights in paragraph 9.1, please contact our Data Protection Contact.

10 Subject access requests

- 10.1 Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When a data subject makes an SAR, we will usually take the following steps:
- (a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);
 - (b) confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;
 - (c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and
 - (d) confirm to the data subject whether or not personal data of the data subject making the SAR are being processed.
- 10.2 If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;
- (f) the right to lodge a complaint with the Information Commissioner's Office (ICO);
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
- (i) where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

10.3 We shall also, unless there is an exemption, provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

10.4 Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

10.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

10.6 If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

11 Individual obligations

11.1 You may have access to the personal information of other members of staff, suppliers and customers or clients of the Company in the course of your

employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 9.1 above.

- 11.2 If you have access to personal information, you must:
 - 11.2.1 only access the personal information that you have authority to access, and only for authorised purposes;
 - 11.2.2 only allow other Company staff to access personal information if they have appropriate authorisation;
 - 11.2.3 only allow individuals who are not Company staff to access personal information if you have specific authority to do so from our Data Protection Contact;
 - 11.2.4 keep personal information secure;
 - 11.2.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
 - 11.2.6 not store personal information on local drives or on personal devices that are used for work purposes.
- 11.3 You should contact our Data Protection Contact if you are concerned or suspect that any breaches of this policy have taken place (or is taking place or likely to take place).

12 Information security

- 12.1 Information may be held at our offices and third party agencies, service providers, representatives and agents and in cloud based IT services.
- 12.2 The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
 - 12.2.1 making sure that, where possible, personal information is pseudonymised or encrypted;
 - 12.2.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 12.2.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
 - 12.2.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 12.3 Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Before any new agreement involving the processing of

personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by our Data Protection Contact.

13 Retention of personal (and sensitive personal) information

- 13.1 Personal information (and sensitive personal information) will be retained in accordance with Schedule 1.
- 13.2 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

14 Data breaches

- 14.1 A data breach may take many different forms, for example:
 - 14.1.1 loss or theft of data or equipment on which personal information is stored;
 - 14.1.2 unauthorised access to or use of personal information either by a member of staff or third party;
 - 14.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;
 - 14.1.4 human error, such as accidental deletion or alteration of data;
 - 14.1.5 unforeseen circumstances, such as a fire or flood;
 - 14.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
 - 14.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.
- 14.2 The Company will:
 - 14.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
 - 14.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

15 International transfers

- 15.1 The Company may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) on the basis that the organisation receiving the information has provided adequate safeguards. Please see the Company's data protection privacy notice for further information.

16 Consequences of failing to comply

- 16.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy puts individuals whose personal information is being processed at risk, carries significant civil and criminal sanctions for the individual and the Company and may, in some circumstances, amount to a criminal offence by the individual.

16.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

16.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact our Data Protection Contact.

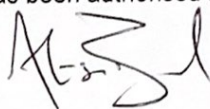
Schedule 1

Type of employment record	Retention period
<p>Recruitment records including but not limited to:</p> <ul style="list-style-type: none"> Completed online application forms or CVs. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) 	<p>Six months after notifying candidates of the outcome of the recruitment exercise.</p>
<p>Immigration checks</p>	<p>Two years after the termination of employment.</p>
<p>Contracts</p>	<p>While employment continues and for six years after the contract ends.</p>
<p>Payroll and wage records</p>	
<p>PAYE records</p>	<p>These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for six years after employment ends.</p>

Other payments	While employment continues and for six years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for six years after the working relationship ends.
Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made.
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for six years after employment ends.
Personnel records	
<p>These may include:</p> <ul style="list-style-type: none"> • Qualifications/references. • Consents for the processing of special categories of personal data. • Annual leave records. • Annual assessment reports. • Disciplinary procedures. • Grievance procedures. • Death benefit nomination and revocation forms. • Resignation, termination and retirement. 	While employment continues and for six years after employment ends.

<ul style="list-style-type: none"> • Working Time Opt Outs 	
Records in connection with working time	
Records to show compliance	Two years after the relevant period.
Maternity records	
<p>These may include:</p> <ul style="list-style-type: none"> • Maternity payments. • Dates of maternity leave. • Period without maternity payment. • Maternity certificates showing the expected week of confinement. 	Three years after the end of the tax year in which the maternity pay period ends.
Accident records	
These are created regarding any reportable accident, death or injury in connection with work.	For at least three years from the date the report was made.
Health Surveillance	
A health record must be kept for all employees under health surveillance as required by the Health & Safety Executive.	For at least 40 years from the date of last entry because often there is a long period between exposure and onset of ill health.

This policy has been authorised by:

Name: ALISON BOND Signed: 

Date: 21.11.22

Director