PRIVACY NOTICE – STAFF DATA

1. What is the purpose of this document?

1.1. Carfax Health Enterprise CIC is committed to protecting the privacy and security of your personal information.

1.2. 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 General Data Protection Regulation (GDPR).

1.3. Carfax Health Enterprise CIC is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

1.4. This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

1.5. It is important that you read 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 such information.

2. Data protection principles

2.1. We will comply with data protection law. This says that the personal information we hold about you must be:

a) Used lawfully, fairly and in a transparent way.
b) Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
c) Relevant to the purposes we have told you about and limited only to those purposes.
d) Accurate and kept up to date.
e) Kept only as long as necessary for the purposes we have told you about.
f) Kept securely.

3. The kind of information we hold about you

3.1. 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 identity has been removed (anonymous data).

3.2. There are "special categories" of more sensitive personal data which require a higher level of protection. Please see 3.4 below.

3.3. We may collect, store, and use the following categories of personal information about you:

a) Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
b) Date of birth.
c) Gender.
d) Marital status.
e) Next of kin and emergency contact information.
f) National Insurance number.
g) Bank account details, payroll records and tax status information.
h) Salary, annual leave, pension and benefits information.
i) Start date.
j) Location of employment or workplace.
k) Copy of passport, driving licence and/or other photographic ID.
l) Copy of birth/adoption, marriage, naturalisation, change of name certificates.
m) Copy of evidence of address, eg bank statement, utility bill.
n) Recruitment information (including copies of right to work documentation, references, interview notes and opinions taken during and following interviews and other information included as part of the application process).
o) Employment records (including job titles, work history, working hours, training records and qualifications).
p) Professional membership registration and record of regular checks for restrictions.
q) Performance information including copies if appraisals.
r) Disciplinary and grievance information.
s) Information about your use of our information and communications systems.
t) Timesheets showing your working pattern, both digital and on paper.
u) Photographs.
v) County Court Judgement, Deduction from Earnings

3.4. We may also collect, store and use the following "special categories" of more sensitive personal information:

a) Information about your race or ethnicity, religious beliefs, sexual orientation and disability.
b) Trade union membership.
c) Information about your health, including any medical condition, health and sickness records including vaccinations.
d) Biometric data specific to the Timebox.
e) Information about criminal convictions and offences.

4. How is your personal information collected?

4.1. We typically collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We also collect additional information from third parties including former employers, or other background check agencies including Disclosure and Barring Service.

4.2. We will collect additional personal information in the course of job-related activities throughout the period of you working for us. This will usually be directly from you but may be from third parties such as medical practitioners.

5. How we will use information about you

5.1. 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 of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

a) Making a decision about your recruitment or appointment.
b) Determining the terms on which you work for us.
c) Checking you are legally entitled to work in the UK.
d) Paying you and, if you are an employee, deducting tax and National Insurance contributions.
e) Providing the following benefits to you:
    - Sick Pay
    - Maternity/Paternity Pay
    - Death in service
    - Pension
    - Expenses reimbursements including Medical Indemnity
    - Annual Leave
f) Liaising with your pension provider.
g) Administering the contract we have entered into with you.
h) Business management and planning, including accounting and auditing.
i) Conducting performance reviews, managing performance and determining performance requirements.
j) Making decisions about salary reviews and compensation.
k) Assessing qualifications for a particular job or task, including decisions about promotions.
l) Gathering evidence for possible grievance or disciplinary hearings.
m) Making decisions about your continued employment or engagement.
n) Making arrangements for the termination of our working relationship.
o) Education, training and development requirements.
p) Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
q) Ascertaining your fitness to work.
r) Managing sickness absence.
s) Complying with health and safety obligations.
t) To monitor your use of our information and communication systems to ensure compliance with our IT policies.
u) To ensure network and information security, including preventing unauthorised access to our computer and electronic communication systems and preventing malicious software distribution.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information. The majority of the above types of processing will be justified on the basis of being necessary to perform a contract and/or so that we comply with a legal obligation. A few will be justified on the basis of legitimate interests.

5.2. In terms of the legitimate interests of Carfax Health Enterprise CIC or of third parties, these legitimate interests will be:
a) to enable us to deal with and defend a dispute or legal proceedings

5.3. We may also use your personal information in the following situations, which are likely to be rare:

a) Where we need to protect your interests (or someone else's interests).
b) Where it is needed in the public interest or for official purposes.

5.4. 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).

5.5. 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.

5.6. 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.

6. How we use particularly sensitive personal information

6.1. "Special categories" of particularly sensitive personal information require higher levels of protection.

6.2. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

a) In limited circumstances, with your explicit written consent.
b) Where we need to carry out our legal obligations and in line with our data protection policy.
c) Where it is needed in the public interest, such as for equal opportunities monitoring, and in line with our data protection policy.
d) Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
e) Where it is necessary for establishing, exercising or defending legal claims.

6.3. Less commonly, we may process this type of information where it is 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.

6.4. We will use your particularly sensitive personal information in the following ways:

a) We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
b) We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
c) We will use information about your gender and ethnic origin, to ensure meaningful equal opportunity monitoring and reporting.

d) We may obtain your biometric data as part of our recruitment process so as to comply with right to work checks.
e) We may use all special categories of data to defend legal claims.

6.5. 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. For example, to ensure we provide you with a safe place of work or to consider making reasonable adjustments. 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.

7. Information about criminal convictions

7.1. We envisage that we will hold information about criminal convictions.

7.2. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

7.3. Checks regarding criminal convictions will be performed by the Disclosure and Barring Service and the information will be provided to us. Currently the checks are performed by MG Care Executive Ltd trading as uCheck.

7.4. We will use information about criminal convictions and offences in the following ways:

a) as part of the recruitment process to establish whether or not to offer you a role.
b) during the working relationship to establish whether you are suitable for continued employment or engagement.

7.5. We are allowed to use your personal information in this way to carry out our obligations under the Rehabilitation of Offenders Act 1974, Children Act 2004, Safeguarding Vulnerable Groups Act 2006. The processing will be in accordance with our data protection policy.

8. Automated decision-making

8.1. Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

8.2. 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.

9. Data sharing

9.1. We may 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.

9.2. "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, HR data including sickness, employment data.

9.3. All our third-party service providers 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.

9.4. We may share your personal information with other third parties, for example in the context of the possible transfer of services. We may also need to share your personal information with a regulator or to otherwise comply with the law.

9.5. We will not transfer the personal information we collect about you outside of the European Union. We will notify you in writing if this position changes.

10. Data Security

10.1. 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. In addition, 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. Details of these measures may be obtained from HR.

10.2. 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.

11. Data retention

11.1. We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of data retention are available in our document retention policy.

11.2. 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, and the applicable legal requirements.

11.3. In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. 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.

12. Rights of access, correction, erasure, and restriction

12.1. 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.

12.2. Under certain circumstances, by law you have the right to:

a) **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

b) **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

c) **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

d) **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.

e) **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

f) **Request the transfer** of your personal information to another party.

12.3. 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 Business Manager in writing.

12.4. You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

12.5. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

13. Right to withdraw consent

13.1. In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Business Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

14. Responsibility for compliance

14.1. Business Manager is responsible for overseeing our compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact Tina McCready. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

15. Changes to this privacy notice

15.1. 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 the Business Manager.