DATA PROTECTION AND PRIVACY NOTICE POLICY

This document sets out the Company's policy on the protection of information relating to staff members, workers, contractors, volunteers and interns (referred to as staff members). Protecting the confidentiality and integrity of personal data is a critical responsibility that the Company takes seriously. The Company will ensure that data is always processed in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR).

KEY DEFINITIONS

Data Processing

Data processing is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Personal Data

Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Company possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Sensitive Personal Data

Sensitive personal data is a special category of information which relates to a data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

PRIVACY NOTICE

This policy constitutes a privacy notice setting out the information the Company holds about staff members, the purpose for which this data is held and the lawful basis on which it is held. The Company may process personal information without staff members' knowledge or consent, in compliance with this policy, where this is required or permitted by law.

FAIR PROCESSING OF DATA

Fair Processing Principles

In processing staff members' data, the following principles will be adhered to. Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes;
- Relevant to specific purposes and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the specified purposes; and
- Kept securely.

Lawful Processing of Personal Data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, the Company will use personal information in the following circumstances:

- when it is needed to perform staff members' contracts of employment;
- when it is needed to comply with a legal obligation; or
- when it is necessary for the Company's legitimate interests (or those of a third party) and staff members' interests and fundamental rights do not override those interests.

The Company may also use personal information in the following situations, which are likely to be rare:

- when it is necessary to protect staff members' interests (or someone else's interests); or
- when it is necessary in the public interest or for official purposes.

Lawful Processing of Sensitive Personal Data

The Company may process special categories of personal information in the following circumstances:

- In limited circumstances, with explicit written consent;
- in order to meet legal obligations;
- when it is needed in the public interest, such as for equal opportunities
- monitoring or in relation to the Company's occupational pension scheme; or
- when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, the Company may process this type of information where it is needed in relation to legal claims or where it is needed to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving consent, or where a staff member has already made the information public. The Company may use particularly sensitive personal information in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leaves, may be used to comply with employment and other laws;
- information about staff members' physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;
- information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting; and
- information about trade union membership may be used to pay trade union premiums, register the status of a protected staff member and to comply with employment law obligations.

Lawful Processing of Information about Criminal Convictions

The Company envisages that it will hold information about criminal convictions. The Company will only use this information where it has a legal basis for processing the information. This will usually be where such processing is necessary to carry out the Company's obligations. Less commonly, the Company may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving consent, or where the staff member has already made the information public.

The Company will only collect information about criminal convictions if it is appropriate given the nature of the role and where it is legally able to do so. Where appropriate, the Company will collect information about criminal convictions as part of the recruitment process or may require staff members to disclose information about criminal convictions during the course of employment.

Consent to Data Processing

The Company does not require consent from staff members to process most types of staff member data. In addition, the Company will not usually need consent to use special categories of personal information in order to carry out legal obligations or exercise specific rights in the field of employment law. If a staff member fails to provide certain information when requested, the Company may not be able to perform the contract entered into with the staff member (such as paying the staff member or providing a benefit). The Company may also be prevented from complying with legal obligations (such as to ensure the health and safety of staff members).

In limited circumstances, for example, if a medical report is sought for the purposes of managing sickness absence, staff members may be asked for written consent to process sensitive data. In those circumstances, staff members will be provided with full details of the information that sought and the reason it is needed, so that staff members can carefully consider whether to consent. It is not a condition of staff members' contracts that staff members agree to any request for consent.

Where staff members have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. Once the Company has received notification of withdrawal of consent it will no longer process information for the purpose or purposes originally agreed to unless it has another legitimate basis for doing so in law.

Automated Decision Making

The Company does not envisage that any decisions will be taken about staff members using automated means, however staff members will be notified if this position changes.

COLLECTION AND RETENTION OF DATA

Collection of Data

The Company will collect personal information about staff members through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. The Company may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

From time to time, the Company may collect additional personal information in the course of job-related activities throughout the period of employment. If the Company requires to obtain additional personal information, this policy will be updated, or staff members will receive a separate privacy notice setting out the purpose and lawful basis for processing the data.

Retention of Data

The Company will only retain staff members' personal information for as long as necessary to fulfil the purposes it was collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

When determining the appropriate retention period for personal data, the Company will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which the personal data is processed, whether the Company can achieve those purposes through other means, and the applicable legal requirements.
In some circumstances the Company may anonymise personal information so that it can no longer be associated with individual staff members, in which case the Company may use such information without further notice to staff members. After the data retention period has expired, the Company will securely destroy staff members' personal information.

DATA SECURITY AND SHARING

Data Security

The Company has put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Details of these measures are available upon request. Access to personal information is limited to those staff members, agents, contractors and other third parties who have a business need to know. They will only process personal information on the Company's instructions and are subject to a duty of confidentiality. The Company expects staff members handling personal data to take steps to safeguard personal data of staff members (or any other individual) in line with this policy.

Data Sharing

The Company requires third parties to respect the security of staff member data and to treat it in accordance with the law. The Company may share personal information with third parties, for example in the context of the possible sale or restructuring of the business. The Company may also need to share personal information with a regulator or to otherwise comply with the law.

The Company may also share staff member data with third-party service providers where it is necessary to administer the working relationship with staff members or where the Company has a legitimate interest in doing so. The following activities are or might be carried out by third-party service providers: payroll, pension administration, benefits provision and administration, and IT services.

STAFF MEMBER RIGHTS AND OBLIGATIONS

Accuracy of Data

The Company will conduct regular reviews of the information held by it to ensure the relevancy of the information it holds. Staff members are under a duty to inform the Company of any changes to their current circumstances. Where a Staff member has concerns regarding the accuracy of personal data held by the Company, the Staff member should contact the HR Manager to request an amendment to the data.

Staff Member Rights

Under certain circumstances, staff members have the right to:

- Request access to personal information (commonly known as a "data subject access request").
- Request erasure of personal information.
- Object to processing of personal information where the Company is relying on a legitimate interest (or those of a third party) to lawfully process it.
- Request the restriction of processing of personal information.
- Request the transfer of personal information to another party.

If a staff member wishes to make a request on any of the above grounds, they should contact the HR Manager in writing. Please note that, depending on the nature of the request, the Company may have good grounds for refusing to comply. If that is the case, the staff member will be given an explanation by the Company.

Data Subject Access Requests (DSAR)

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

The Company may need to request specific information from the staff member to help confirm their identity and ensure the right to access the information (or to exercise any of the 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.

COMPLIANCE WITH THIS POLICY

The Company's Responsibility for Compliance

If applicants have any questions about this policy or how the Company handles personal information, they should contact the MD.

Additionally, staff 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.

Data Security Breaches

The Company has put in place procedures to deal with any data security breach and will notify staff members and any applicable regulator of a suspected breach where legally required to do so. Details of these measures are available upon request.

In certain circumstances, the Company will be required to notify regulators of a data security breach within 72 hours of the breach. Therefore, if a staff member becomes aware of a data security breach it is imperative that they report it to DPC immediately.

Privacy by Design

The Company will have regard to the principles of this policy and relevant legislation when designing or implementing new systems or processes (known as "privacy by design").
Staff Members' Responsibility for Compliance

All staff members, particularly those tasked with regularly handling personal data of colleagues or third parties, have responsibility for ensuring that processing meets the standards set out in this policy. Staff members should observe, as a minimum, the following rules:

- Staff members must observe any instruction or guidelines issued by the Company in relation to data protection.
- Staff members should not disclose personal data about the Company, colleague or third parties unless that disclosure is fair and lawful, in line with this policy;
- Staff members must take confidentiality and security seriously, whether the staff member considers the information to be sensitive or not.
- Any personal data collected or recorded manually which is to be inputted to an electronic system should be inputted accurately and without delay.
- Staff members must not make any oral or written reference to personal data held by the Company about any individual except to staff members of the Company who need the information for their work or an authorised recipient.
- Great care should be taken to establish the identity of any person asking for personal information and to make sure that the person is entitled to receive the information.
- If a staff member is asked by an unauthorised individual to provide details of personal information held by the Company the staff member should ask the individual to put their request in writing and send it to the HR Manager. If the request is in writing the staff member should pass it immediately to the HR Manager.
- Staff members must not use personal information for any purpose other than their work for the Company.
- If a staff member is in doubt about any matter to do with data protection they must refer the matter to their line manager immediately.
- Passwords should not be disclosed and should be changed regularly;
- Staff member or third-party personal data should not be left unsecured or unattended, e.g. on public transport;
- Unauthorised use of computer equipment issued by the Company is not permitted;
- Staff members should maintain a "clear desk" and ensure that all personal and sensitive employee information, is secured when it is not in use or when the staff member is not at work;
- Staff members may use only encrypted Company equipment to carry out work and must ensure that devices are password protected and locked when not in use. Staff must not store any staff member or third-party personal data locally on their device;
- Emails containing staff member, or third-party personal data must not be sent from a web-based email system;
- As far as possible, staff member or third-party personal data contained in emails and attachments should be anonymised before it is sent by email; and

- Consideration should be made where documents contain sensitive information, if they should be password protected and, if the document requires to be transmitted, the document and password should be transmitted separately.

Any breach of the above rules will be taken seriously and, depending on the severity of the matter, may constitute gross misconduct which could lead to summary termination of employment.

Other useful information can be found in the ICO.Org.UK Website under GDPR.

SIGNED

John Morrison (MD) 01/11/2022

DATE	REVISION	DETAIL	PREPARED BY	APROVED BY
July 2020	A	New background	John Morrison	John Morrison
November 2021	B	Review – No Change	John Morrison	John Morrison
November 2022	B	Annual Review	John Dunn	John Morriosn