ELWELL WATCHORN & SAXTON LLP

PRIVACY NOTICE - STAFF MEMBER AND JOB APPLICANT

This document sets out in detail the policy of Elwell Watchorn & Saxton LLP ("the Company") on the protection of information relating to staff members, workers, contractors, volunteers and interns (referred to as Staff Members) and those applying for such positions (Job Applicants). Protecting the confidentiality and integrity of personal data is a critical responsibility that the Company takes seriously at all times. The Company will ensure that data is always processed fairly, in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

KEY DEFINITIONS

Data processing

Data processing is any activity that involves the use of personal data. It includes obtaining, recording or holding information, or carrying out any operation or set of operations, 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 by which a living person to whom the data relates can be identified. 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, such as a disciplinary record. There are also "special categories" of more sensitive personal data which require a higher level of protection. Information about criminal convictions is also afforded higher levels of protection.

The Company necessarily collects personal data about its Staff Members and Job Applicants and this Privacy Notice explains how we treat that personal data and your rights in relation to it.

PRIVACY NOTICE

This document is the Company's Staff Member and Job Applicant Privacy Notice, it explains your rights in detail. This notice, together with the information contained in the Data Processing Register, sets 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.

The Staff Member and Job Applicant Privacy Notice will be made available to Staff Members upon joining the Company and to job applicants by way of a link in any on line job advertisement. The Data Processing Register is available on request. If the purpose for processing any piece of data about Staff Members should change, the company will update the Staff Member and Job Applicant Privacy Notice and Data Processing Register with the new purpose(s) and the lawful basis for processing the data and will notify all Staff Members by email.

FAIR PROCESSING PRINCIPLES

In processing Staff Members' and Job Applicants' personal 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.

COLLECTION AND RETENTION OF DATA

How is your personal information collected?

The Company will collect personal information about Staff Members and Job Applicants 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 such as referees or 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.

What information is collected about you?
We may 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 and dependents;
- 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 and leaving dates;
- Location of employment or workplace;
- 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, training records and professional memberships);
- Compensation history;
- Performance information;
- Disciplinary and grievance information;
- Information about your use of our information and communications systems;
- Photographs;

In limited circumstances, we may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions;
- Trade union membership;
- Information about your health, including any medical condition, health and sickness records;
- Genetic information and biometric data;
- Information about criminal convictions and offences;

How is information about you used?
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
- less commonly, 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 (such as in connection with monitoring visits from our regulatory bodies.

A list of each category of personal data we hold and the lawful basis we believe the Company to have for processing it may be found in the Data Processing Register.

The situations in which we envisage using your personal information are as follows:

- Making a decision about your recruitment or appointment;

- Determining the terms on which you work for us;
- Checking you are legally entitled to work in the UK;
- Paying you and, if you are an employee, deducting tax and National Insurance contributions;
- Providing the following benefits to you:
- Death in service benefit;
- Pension benefits;
- Liaising with your pension provider;
- 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 continuing professional 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, money laundering or terrorist financing;
- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- 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;
- Equal opportunities monitoring.

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.

Special categories (sensitive) personal data
Some categories of personal data are considered by law to be particularly sensitive and are therefore classed as “special categories” of personal data. These relate to a person’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. This type of data is afforded additional protection.

What constitutes special categories of data and how it is processes and protected is explained in greater detail in our Special Category Data Policy.

In summary, the Company may process special categories of personal information in the following circumstances:

- primarily, when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards; or
- in order to meet legal obligations (for instance in calculating your entitlement to sick pay or maternity pay); or
- 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
- In limited circumstances, with explicit written consent, such as the inclusion of your photograph on our website or in marketing material;

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 will typically use special categories of 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;

Additionally, the Company may occasionally use sensitive personal information in the following ways:

- 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.

Information about criminal convictions

The Company envisages that it may hold information about criminal convictions where these are relevant to the performance of the functions of an insolvency Office Holder. If it becomes necessary to do so, 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 of the employee and where it is legally able to do so. Relevant convictions would typically be those relating to theft, fraud or dishonesty by a Staff Member and/or that would otherwise bring discredit upon the Company and/or undermine the Company's ability to perform functions associated with the professional practice of insolvency administration.

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.

How long is information about you kept?

Information about unsuccessful Job Applicants is retained for 6 months from the date of the application, unless you specifically request its destruction.

The retention period for information about Staff Members depends upon the nature of the information. 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, regulatory, accounting, or reporting requirements. Details of retention periods for different aspects of personal information are set out in the Data Processing Register and Data Retention Policy.

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.

Consent to data processing
The Company does not require consent from Staff Members to process most types of personal data. In addition, the Company will not usually need consent to use special categories of personal data or information about criminal convictions in order to carry out legal obligations or exercise specific rights in the field of employment law.

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

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 contained in our Confidentiality and Data Security Policy.

In summary, 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 in line with this and the Confidentiality and Data Security Policy and disciplinary action or termination of contract may arise from a breach of confidentiality and/or data security.

Data sharing
The Company requires third parties to respect the security of Staff Member data and to treat it in accordance with the law. Personal data about Staff Members will only be shared if it is lawful and necessary.

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 carried out by third-party service providers:

Name of company / Organisation	Service provided
EACS	IT support services
MHA MacIntyre Hudson	Accountancy services
Bray & Bray	Legal Services

Occasionally, we may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Transfer of data outside the EU
We do not anticipate the transfer of your data outside the EU. The Company holds personal data in its physical files and on its Microsoft Azure servers. You will be notified in the event the Company intends to transfer your data outside of the EU.

STAFF MEMBERS' RIGHTS
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 Office Manager to request an amendment to the data.

Staff members' 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 their Line 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.

Accessing the information that we hold
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 DATA PROTECTION
The Company's responsibility for compliance
Given the size of the Company, it has not been deemed necessary to formally appoint a Data Protection Officer. Oversight of data privacy throughout the Company and its operations rests collectively with our Partners.

In insolvency cases, ultimate responsibility rests with the named Licensed Insolvency Practitioner that has been appointed in respect of an insolvent entity's affairs.

If Staff Members have any questions about this policy or how the Company handles personal information, they should contact their line manager in the first instance. Staff Members 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 contained in the Company's Data Breach Policy.

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, or suspects a data breach may have occurred, it is imperative that they report it immediately, in accordance with the Data Breach Policy.

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"). The importance of data privacy has already been reflected and incorporated into the following policies, processes and notices, which are available to all within the Staff Intranet area:

GDPR Policies:

- Confidentiality and Data Security Policy
- Data Breach Policy
- Data Retention and Destruction Policy
- Data Subject Access Policy
- Privacy Notices for:
  - Staff members and job applicants [this document]
  - Business contacts and customers
  - Debt advice and personal insolvency clients
  - Directors, shareholders and owners of insolvent businesses
  - Creditors, book debtors and employees of insolvent businesses (Stakeholders)
- Special Category Data Policy
- Supplier Oversight Policy
- Vulnerable Clients Policy

Staff Handbook Policies:

- Absence Policies and Procedures
- Information Systems
- How to resolve a problem at work
- Employee Development
- Other Arrangements

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 and other relevant policies. All staff members should familiarize themselves with and observe the above policies, and any others that may be implemented from time to time.

Staff members are invited to raise any concerns that have about the privacy of their own data, or the data of colleagues, customers or any other persons with whom the Company interacts, with their Line Manager, or any of the Partners.

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.

CHANGES TO THIS PRIVACY NOTICE
The Company reserves 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 your Line Manager or any of the Partners.