Data Protection and Security Policy

The Employer is committed to ensuring that the personal data of our Employees is handled in accordance with the relevant data protection legislation.

This policy sets out what you should expect when we collect your personal information and how we will process it. This policy should be read in conjunction with other Employer policies and procedures.

We reserve the right to update this policy from time to time. Where appropriate, we will provide substantial updates to you for any additional activities not mentioned in this policy.

How do we get your information?

We get your personal information from the following sources:

- Directly from you;
- From an employment agency;
- From your previous employer;
- From security clearance and background check providers;
- If you are a secondee, from your employer;
- From Occupational Health and other health providers;
- From Pension administrators, HMRC and other government departments;
- From your Trade Union (if applicable); and
- From providers of Employee benefits.

What personal data do we process and why?

We collect and process the following information in relation to your employment to carry out the contracts we have with you:

- **Personal Contact Details** including your name, residential address, personal mobile and telephone numbers and personal email address.
- **Sensitive Information** including your date of birth, gender, National Insurance number, a copy of your passport or similar photographic identification, criminal record or security clearance details.
- **Emergency Contact Details** of your next of kin, emergency contacts and their contact information such as their name, address, personal mobile and telephone numbers.
- **Employment History** including your job application to the Employer, employment references, previous roles and employers.
- **Educational History** including your qualifications and copies of your school and/or university degree certificates.
- **Declarations** in relation to any conflict of interest, gifts, secondary employment, political, intellectual property or criminal convictions that you declare to us.
- **In relation to your job role** including start and leave dates, changes to your employment contract, hours worked, targets and duties, requests for flexible working, details of any sick leave, and content produced for use on our website or social media such as photographs, videos, authored articles, blog posts and speech transcripts.
- **In relation to your salary, pension and loans** including any changes to your salary, bonus or commission entitlements, expenses, loans such as for travel season tickets, details of any paid or unpaid leave, pension details, bank account details, payroll records and tax status.

- **In relation to your performance and training** including probation reviews, annual reviews, promotions, poor performance complaints, grievance matters and investigations, disciplinary records, whistleblowing concerns raised by you or which you may have been party to and training history.
- **In relation to your health and wellbeing (other special category data)** including such data either declared by you or obtained from a medical expert with your consent, sick leave forms, health management questionnaires or fit notes, occupational health referrals and reports, accident at work records, information you have provided regarding Protected Characteristics as defined by the Equality Act for the purpose of equal opportunities monitoring.
- **In relation to monitoring** including about your access controls, derived from monitoring IT acceptable use standards and CCTV images taken using our own CCTV systems (if such systems are in use).
- Except where anonymised, your response to Employee surveys.

Lawful basis for processing your personal data

Depending on the processing activity as outlined above, we rely on the following lawful basis for processing your personal data:

- it being necessary for the performance of a contract with you;
- so we can comply with our legal obligations as your employer;
- in order to protect your vital interests or those of another person;
- for the performance of our public task; or
- for the purposes of our legitimate interest

Where the personal data we process is special category data, for example your identification documents or health data, the additional basis for processing that we rely on are:

- carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights;
- to protect your vital interests or those of another person where you are incapable of giving your consent;
- for the establishment, exercise, or defence of legal claims; or
- for archiving purposes in the public interest.

We also rely on Schedule 1 (part 1, paragraph 1) of the Data Protection Act 2018 ("**DPA 2018**"), which relates to the processing of special category data for employment purposes.

Where the personal data we process is in relation to criminal convictions and offences, the lawful basis for processing that we rely on are:

- for the performance of our public task; or
- for the performance of a contract.

We also rely on Schedule 1 (part 2, paragraph 6(2)(a)) of the DPA 2018.

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our Privacy Notice.

How long do we keep your personal data for?

For information on how long we retain your personal data and how we securely dispose of your personal data once it has expired, please ask your manager for more information on the Employer's document retention guidelines.

Who do we share your personal data with?

We may share your personal data with third parties including our data processors (a list of our current data processors can be found at ANNEX A), government agencies (such as HMRC for the purpose of collecting tax and national insurance) and external auditors.

We may be legally obliged to share your personal data under a Court Order.

Before we share your personal data with any third party, we ensure we have a written agreement in place with them, allowing them to process your personal data for specified purposes only and in accordance with our written instructions. We ensure they have appropriate security measures to protect your personal data in line with this policy and further, we do not permit any third party that we are contracted with to use your personal data for their own purposes.

In the event we must transfer Employee personal data outside of the EU/EEA, we will ensure that appropriate safeguards and adequate security measures are in place to ensure your personal data is safe. Before transferring Employee personal data outside of the EU/EEA we will ensure the importer has adequate levels of protection and appropriate security measures in place to ensure your personal data is safe. If you would like further information about this, please speak with your manager.

Automated Decision-Making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We do not envisage that any decisions will be taken about you using automated means, however where you will be subject to decisions that will have a significant impact on you based solely on automated decision-making, we will on process data in such a way where we have a lawful basis for doing so and we have notified you in writing.

Our Data Security Commitments

We hold your physical and electronic records securely on our servers and at our premises. General Employees cannot gain access to this data. The data is only available to a small number of Employees who are responsible for running or administrating certain functions. If you would like to request what personal data of yours is kept by the Employer please submit a request to your manager.

We have implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by processing your personal data and to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way. We ensure that anyone who has access to your personal data is acting under authority and does not process it except on express written instructions.

We have appropriate 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.

Your Data Security Commitments

Equipment Security and Passwords

You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.

You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

Data Security

You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

You must not download or install software from external sources without authorisation. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation.

We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

Inform your manager immediately if you suspect your computer may have a virus.

Monitoring Employees

We are committed to respecting Employee privacy concerning their use of the Employer’s IT systems and equipment; however, we reserve the right to log and monitor such use.

Breach of this policy may result in disciplinary action up to and including dismissal.

Use of the Employer's Systems

We allow you to use our internal and online systems to send personal e-mails, browse the internet for personal reasons and make personal telephone calls using work telephones, subject to certain conditions. Personal use is a privilege and not a right and it must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

We are able to monitor telephone, e-mail, voicemail, internet and other communications on our systems. We occasionally monitor your use of our systems for business reasons, and in order to carry out legal obligations in our role as an employer.

We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, to investigate an alleged wrongdoing and to comply with any legal obligation.

CCTV

We may operate CCTV inside and outside of our premises to monitor access to certain areas of the office and to maintain a safe and secure working environment for all Employees and visitors. Particularly we believe the use of CCTV is necessary for legitimate business purposes, for example, to assist:

- the prevention of crime and protection of the office building and assets within the building;
- the personal safety and day-to-day management of Employees and visitors; and
- and support law enforcement.

All personal data recorded by use of CCTV is processed by Employees who have been approved to view the images and in accordance with data protection laws.

Personal data recorded by the CCTV will be retained in accordance with our document retention guidelines.

We may share personal data captured by the CCTV where we consider it is reasonably necessary for any of the legitimate purposes set out above.

You may make a request for disclosure of your personal data obtained by the use of CCTV by submitting a data subject access request as described below.

Your Rights as a Data Subject

Under certain circumstances, you have the right to:

- Request access to your personal information.

- Request correction of the personal data that we hold about you.
- Request erasure of the personal data that we hold about you.
- Object to processing of your personal data where we are relying on a legitimate interest.
- Request the restriction of processing your personal data.
- Request the transfer of your personal data.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact your manager.

If you have any questions about this policy or how we handle your personal data, please contact your manager. You also 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.