# Data Protection Policy

**Introduction**

The Company takes the security and privacy of your data seriously. The Company needs to gather and use information or 'data' about you as part of the business and to manage the relationship with you. The Company intends to comply with its legal obligations under the Data Protection Act 2018 (the '2018 Act') and the UK General Data Protection Regulation ('GDPR') in respect of data privacy and security. The Company has a duty to notify you of the information contained in this policy.

This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company. This policy applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice the Company issues to you from time to time in relation to your data.

The Company has separate policies and privacy notices in place in respect of customers, suppliers and other categories of data subject. A copy of these can be obtained from your Manager.

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

Reference to the Data Protection Manager is the person who is responsible for Data Protection on a day to day basis.

**Definitions**

**Personal data -** is information which relates to a living person who can be identified from that data on its own, or when taken together with other information.

**Data subject -** if you are a current or former employee, worker, volunteer, apprentice or consultant then you are a 'data subject' for the purposes of this policy.

**Data controller -** the Company is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of processing personal data.

**Processing -** is any use of data, including collecting, storing, amending, disclosing or destroying it.

**Data Protection Principles**

The Company processes personal data in accordance with the following data protection principles and commits that personal data will:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;

- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed;
- be processed securely.

**Personal Data**

**Personal data** is any information that relates to an individual who can be identified from that information. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials. Personal data may be provided to the Company by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by the Company. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

**Types of Personal Data**

The Company will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- any other category of personal data which we may notify you of from time to time;

- any criminal convictions and offences (see below).

**Special Categories of Personal Data**

Special categories of personal data are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health; and
- your sex life and sexual orientation.

The Company may hold and use any of these special categories of your personal data in accordance with the law.

The Company does not need your consent to process special categories of your personal data when it is processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims;
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

In particular, the Company may use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- criminal records if we take out DBS checks in order to protect the interests of other employees or the business.

The Company will use information in relation to:

- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety.

**Processing Data**

Processing means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;

- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination;
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

The Company will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for the Company's legitimate interests (or for the legitimate interests of someone else). However, the Company can only do this if your interests and rights do not override ours (or theirs).

You have the right to challenge the Company's legitimate interests and request that the Company stop this processing. See details of your rights in the section below.

The Company can process your personal data for these purposes without your knowledge or consent. The Company will not use your personal data for an unrelated purpose without telling you about it and the legal basis that the Company intends to rely on for processing it.

If you choose not to provide the Company with certain personal data, you should be aware that the Company may not be able to carry out certain parts of the contract between us. For example, if you do not provide the Company with your bank account details, the Company may not be able to pay you. It might also stop the Company from complying with certain legal obligations and duties which it has, such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

The Company does not take automated decisions about you using your personal data or use profiling in relation to you.

The Company may also process information about criminal convictions by way of DBS checks (or Scottish Disclosure check in Scotland). The Company does this as it has a duty of care to our clients and employees of the business, as it is important that the Company knows about anything that may put those people at any kind of risk. The Company therefore have a legitimate interest in carrying out these checks.

**Sharing your Personal Data**

Sometimes the Company might share your personal data with group companies or our contractors and agents to carry out its obligations under the Company's contract with you or for its legitimate interests.

The Company require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Third parties that the Company uses are available on request.

The Company does **not** send your personal data outside the United Kingdom. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

**Individual Obligations**

Everyone who works for, or on behalf of the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.

The Company's Data Protection Manager is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained and you must not share personal data informally.

You are responsible for keeping personal data secure and should avoid making unnecessary copies of data and ensuring that you keep and dispose of any copies securely. Any data which you deal with should be regularly reviewed and updated to ensure that the data remains as accurate as possible. This includes notifying the Company if your own details change.

**Security of Data**

All employees are expected to take all reasonable precautions and follow Company policy and best practice to ensure the security and integrity of personal data held and processed by the Company.

All personal data held in paper format should be kept in locked drawers and filing cabinets. You must not leave paper with personal data unsecure (lying about on desks etc), nor should you take personal data away from the Company's premises without the explicit permission of your Manager or the Data Protection Officer / Manager. Personal data should be shredded and disposed of securely when you have finished with it.

You are expected to observe and implement strong passwords to protect electronically held personal data and should ensure that your computer screen is locked when you are not at your desk. Personal data must not be saved to your own personal computers or other devices. Where practicable, personal data should be encrypted before being transferred electronically. Personal data should never be transferred outside the United Kingdom except in compliance with the law and authorisation of the Data Protection Manager. Further information on encryption is available from the IT Department.

If you are required to collect and hold specific data, including historical data, for statistical or monitoring purposes, you should consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

You should ask for help from our Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with the Company's Disciplinary Procedures. Serious breaches may be considered to be gross misconduct.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under our Disciplinary Procedure, which could result in your dismissal.

**Impact Assessments**

Some of the processing that the Company carries out may result in risks to privacy. Where processing would result in a high risk to your rights, the Company will carry out a data protection

impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks to you and the measures that can be put in place to mitigate those risks.

**Data Breaches**

The Company has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else), then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then the Company must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach **you must** contact the Data Protection Manager immediately and keep any evidence you have in relation to the breach.