Data Protection

What this policy covers

This policy applies to employees, workers and contractors.

This policy details your rights and obligations in relation to your personal data and the personal data of third parties that you may come into contact with during the course of your work.

"Personal data" is any information that relates to a living individual who can be identified from that information.

"Processing" is any use that is made of personal data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or political beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

If you have access to the personal, special categories or criminal records data of staff or of third parties, you must comply with this Policy. Failure to comply with the Policy and procedures may result in disciplinary action up to and including dismissal without notice.

Data Protection principles

The Company processes HR-related personal data in accordance with the following data protection principles:

- the Company processes personal data lawfully, fairly and in a transparent manner;
- the Company collects personal data only for specified, explicit and legitimate purposes;
- the Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of the processing;
- the Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- the Company retains personal data only for the period necessary for the processing;
- the Company adopts appropriate measures to make sure that personal data is secure and is protected against unauthorised or unlawful processing and from accidental loss, destruction or damage.

Your entitlements

Data protection legislation prescribes the way in which the Company may collect, retain and handle personal data. The Company will comply with the requirements of data protection legislation and anyone who handles personal data in the course of their work must also comply with it.

The Company will inform individuals of the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data about individuals for other reasons.

Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the rules relating to special categories of data and criminal records data.

The Company will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment or engagement of an employee, worker, contractor, volunteer, or intern is held in the individual's personal file (in hard copy or electronic format, or both), and on HR systems. The periods for which the Company holds HR-related personal data are contained in its privacy notices.

Access to your personal data [subject access requests]

You have the right to make a subject access request. If you make such a request, the Company will tell you:

- whether or not your data is processed and if so why; the categories of personal data concerned and the source of the data if it is not collected from you;
- to whom your data may be disclosed, including any recipients located outside the UK and the safeguards that apply to any such transfers;
- for how long your personal data is stored or how that period is decided;
- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the Company has failed to comply with your data protection rights; and
- whether or not the Company carries out any automated decision-making and the logic involved in such decision-making.

The Company will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made the request electronically, unless you request otherwise.

If you want additional copies, the Company will charge a fee, which will be based on the administrative cost of providing the additional copies.

Other rights

You have a number of other rights in relation to your personal data. You can require the Company to:

- rectify inaccurate data;
- stop processing or erase data if your interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a lawful basis for processing data);
- stop processing or erase data if it is unlawful; and
- stop processing data for a period if it is inaccurate or if there is a dispute about whether or not your interests override the Company's legitimate interests for processing the data.

Your responsibilities

You are responsible for helping the Company keep your personal data accurate and up to date. You should let the Company know if personal data provided to the Company changes, for example, if you change bank or move house.

You may have access to the personal data of other individuals and of our customers or clients in the course of your employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the Company relies on you to help meet its data protection obligations.

If you have access to personal data, you are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access including password protection, and secure file storage and destruction);
- not to remove personal data or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failure to observe these requirements may amount to a disciplinary offence which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to your dismissal without notice.

Processing special categories and criminal records data

The Company will process special categories and criminal records data primarily where it is necessary to enable the Company to meet its legal obligations and in particular to ensure adherence to health and safety legislation; vulnerable groups protection legislation; or for equal opportunities monitoring purposes.

Procedure

The Company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of data protection legislation.

Personal data relating to staff may be collected by the Company for the purposes of:

- 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;
- 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 development requirements;
- dealing with possible 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;
- to monitor your use of our information and communication systems to ensure compliance with our policies;
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- to record digital meetings to allow replay or storage;
- to conduct data analytics studies to review and better understand employee retention and attrition rates, and
- 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.

How we use special categories and criminal records data

"Special categories" data and "criminal records" data require higher levels of protection. We need to have further justification for collecting, storing and processing these types of personal data. We may process special categories or criminal records data in the following circumstances:

- in limited circumstances, with your explicit written consent;
- where we need to carry out our legal obligations;

- where it is needed in the public interest, such as for equal opportunities monitoring, or in relation to our occupational pension scheme;
- where it is needed to assess your working capacity on health grounds.

Less commonly, we may process this type of data where it is needed in relation to legal claims or where it is needed to protect your vital interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Accuracy of personal data

The Company will review personal data regularly to ensure that it is accurate, relevant and up to date.

To ensure the Company's files are accurate and up to date, and so that the Company is able to contact you or, in the case of an emergency, another designated person, you must notify the Company as soon as possible of any change in your personal details (e.g. change of name, address, telephone number, loss of driving licence where relevant, next of kin details, etc).

Security of personal data

The Company will ensure that personal data is not processed unlawfully, lost or damaged. If you have access to personal data during the course of your employment, you must also comply with this obligation. If you believe you have lost any personal data in the course of your work, you must report it to your manager immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

Data breaches

The Company will record all data breaches regardless of their effect.

If we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about the likely consequences of the breach and the mitigation measures we have taken.

Access to personal data ["subject access requests"]

To make a subject access request, you should send your request to the Company. In some cases, the Company may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require.

We will normally respond to a request within one month from the date we receive it. In some cases, such as where the Company processes large amounts of the individual's data, we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.