

Employee Privacy Notice

- The Company is fully aware of its obligations under the General Data Protection Regulation (GDPR) and is committed to processing your data securely and transparently.
- This privacy notice sets out, in line with GDPR, the types of data that we hold on you as an employee of the Company. It also sets out how we use that information, how long we keep it for and other relevant information about your data.
- This notice applies to current and former employees, workers and contractors.

Data controller details

The Company is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are as follows:

[insert name and contact details of Company]

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way;
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you;
- only use it in the way that we have told you about;
- ensure it is correct and up to date;
- keep your data for only as long as we need it;
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed.

Types of data we process

We may hold many types of data about you, including **[delete and add points from the list as appropriate]**:

- your personal details including your name, address, date of birth, email address, phone numbers;
- your photograph;
- gender;
- marital status;
- dependants, next of kin and their contact numbers;
- medical or health information including whether or not you have a disability;
- information used for equal opportunities monitoring about your sexual orientation, religion or belief and ethnic origin;
- information included on your CV including references, education history and employment history;
- documentation relating to your right to work in the UK;
- driving licence;

- bank details;
- tax codes;
- National Insurance number;
- current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment with us;
- letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings;
- internal performance information including measurements against targets, formal warnings and related documentation with regard to capability procedures, appraisal forms;
- leave records including annual leave, family leave, sickness absence etc;
- details of your criminal record;
- training details;
- CCTV footage;
- building entry card records.

How we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you would normally include in a CV, Application Form or a recruitment cover letter, or notes made by our staff during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in personnel files or within the Company's HR/Personnel and IT systems.

Why we process your data

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment contract that we are party to;
- in order to carry out legally required duties;
- in order for us to carry out our legitimate interests;
- to protect your interests; and
- where something is done in the public interest.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to:

- carry out the employment contract that we have entered into with you; and
- ensure you are paid.

We also need to collect your data to ensure we are complying with legal requirements such as:

- ensuring tax and National Insurance is paid;
- carrying out checks in relation to your right to work in the UK; and
- making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of the Company. We have set these out below:

- making decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc;

- making decisions about salary and other benefits;
- providing contractual benefits to you;
- maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained;
- effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises;
- offering a method of recourse for you against decisions made about you via a grievance procedure;
- assessing training needs;
- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments;
- gaining expert medical opinion when making decisions about your fitness for work;
- managing statutory leave and pay systems such as maternity leave and pay etc;
- business planning and restructuring exercises;
- dealing with legal claims made against us;
- preventing fraud;
- ensuring our administrative and IT systems are secure and robust against unauthorised access.

[insert other legitimate interests as appropriate]

Special categories of data

Special categories of data are data information relating to an individual's:

- health;
- sex life;
- sexual orientation;
- race;
- ethnic origin;
- political opinion;
- religion;
- trade union membership;
- genetic and biometric data.

We must process special categories of data (**where they are held**) in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing;
- we must process the data in order to carry out our legal obligations;
- we must process data for reasons of substantial public interest;
- you have already made the data public.

We will use your special category data:

- for the purposes of equal opportunities monitoring;
- in our sickness absence management procedures;
- to determine reasonable adjustments.

[insert other reasons as appropriate]

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the content and the reasons for the processing.

As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data

The Company is responsible for the care and safeguarding of some of the most vulnerable people in society.

This responsibility is undertaken through its workforce of devoted and dedicated individuals who show exemplary qualities of care and compassion. Our ability to feel confident that our employees possess these, and other important qualities, is because we take our recruitment seriously. This includes exercising sound judgement, and undertaking checking procedures available to and required of us, such as taking up references, confirming qualifications and experience, and ensuring that no individual offered employment with us has either a criminal record which is serious enough for us to withdraw or is someone who is on a list of individuals who are barred from working with vulnerable adults or children, and whose employment would be illegal. Criminal record checks, together with checks on barred lists, are made through the Disclosure and Barring Service (DBS). The Company will request relevant DBS checks on all prospective employees occupying qualifying positions.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract of employment. If you do not provide us with the data needed to do this, we will be unable to perform those duties e.g. ensuring you are paid correctly. We may also be prevented from confirming, or continuing with, your employment with us in relation to our legal obligations if you do not provide us with this information e.g. confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

Sharing your data

Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties. This includes, for example, your line manager for their management of you, maintaining of personnel records and for administering payment under your contract of employment.

We share your data with third parties in order to **[insert details e.g. obtain references as part of the recruitment process]. [You should also specify here any third parties which process data on your behalf e.g. payroll companies and explain why].**

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such. We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such. The Company's policy on the storage/access, handling, usage, retention and disposal of information in relation to criminal records is contained within the policy document "Handling Disclosure Information".

Where we share your data with third parties, we provide written instructions to them to ensure that your data are held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Retention periods can vary depending on why we need your data, as set out below:

[Include details of document retention periods]

Automated decision making

[Select from the following sentences and delete as appropriate]

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

OR

We will make some decisions about you based on automated decision making (where a decision is taken about you using an electronic system without human involvement). [Include more information on this, including the decisions that are taken based on automated decision making, how the decisions are made, the significance of the decisions and the impact that it will have on the data subject].

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice;
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request. You can read more about this in our Subject Access Request policy which is available from a member of the Management Team.
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it;
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it;
- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct;
- the right to portability. You may transfer the data that we hold on you for your own purposes;
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests;
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact a member of the Management Team.

Making a complaint

We hope that we can resolve any query or complaint you raise about our use of your information, so please contact the management team in the first instance.

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, and you wish to take any matter further, then you are able to make a complaint to the ICO

[Delete following paragraph as applicable]

Data Protection Officer

The Company's Data Protection Officer is [insert name]. [Delete as appropriate – He/She] can be contacted on [insert contact details].

Version number: