Data Protection Policy for Employees, Workers & Consultants

1 Overview

1.1 The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018**(the '2018 Act') and the **EU General Data Protection Regulation**('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 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 we issue to you from time to time in relation to your data.

1.3 [The Company has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. A copy of these can be obtained from [insert].]

1.4 The Company has measures in place to protect the security of your data in accordance with our Data Security Policy. A copy of this can be obtained from [insert name].

1.5 The company will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from Sharon Young. We will only hold data for as long as necessary for the purposes for which we collected it.

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

1.7 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.

1.8 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.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- 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; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. 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.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, or someone else such as a former employer, your doctor, or a credit reference agency, or it could be created by us. 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.

3.4 We 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;
- Finger print registration;
- any other category of personal data which we may notify you of from time to time.

4 How we define special categories of personal data

4.1 '**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;
- your sexual orientation; and
- any criminal convictions and offences.

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

5 How we define processing

5.1 **'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; and
- restriction, destruction or erasure.

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

6 How will we process your personal data?

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

6.2 We 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 our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

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

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have 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.

7 Examples of when we might process your personal data

7.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

7.2 For example (and see section 7.6 below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law & other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;

- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*; and
- for any other reason which we may notify you of from time to time.

7.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Sharon Young.

7.4 We do not need your consent to process special categories of your personal data when we are 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; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

7.5 We might process special categories of your personal data for the purposes in paragraph 7.2above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- 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; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

7.6 We do not take automated decisions about you using your personal data or use profiling in relation to you.

8 Sharing your personal data

8.1 Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

8.2 We 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.

8.3 Third parties Elizabeth Canning Payroll manager, NEST pension provider

8.4 We do not send your personal data outside the European Economic Area. 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.

9 How should you process personal data for the Company?

9.1 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.

9.2 The Company's Data Protection named person **[Les Aikman]** 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.

9.3 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.

9.4 You should not share personal data informally.

9.5 You should keep personal data secure and not share it with unauthorised people.

9.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

9.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

9.8 You should use strong passwords.

9.9 You should lock your computer screens when not at your desk.

9.10 Personal data should be encrypted before being transferred electronically to authorised external contacts.

9.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

9.12 Do not save personal data to your own personal computers or other devices.

9.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law.

9.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

9.15 You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.

9.16 Personal data should be shredded and disposed of securely when you have finished with it.

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

9.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

9.19 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

10 How to deal with data breaches

10.1 We have 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 we must also notify the Information Commissioner's Office within 72 hours.

10.2 If you are aware of a data breach you must contact Sharon Young immediately and keep any evidence you have in relation to the breach.

11 Subject access requests

11.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection named person who will coordinate a response.

11.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to Sharon Young. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

11.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

12 Your data subject rights

12.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

12.2 You have the right to access your own personal data by way of a subject access request (see above).

12.3 You can correct any inaccuracies in your personal data. To do you should contact Sharon Young.

12.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Sharon Young.

12.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Sharon Young.

12.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

12.7 You have the right to object if we process your personal data for the purposes of direct marketing.

12.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

12.9 With some exceptions, you have the right not to be subjected to automated decision-making.

12.10 You have the right to be notified of a data security breach concerning your personal data.

12.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Sharon Young.

12.12 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Data Protection Breach Reporting & Procedure

POLICY STATEMENT

The Company is committed to handling personal data in line with best practice and as such this Policy details the procedures to use when dealing with and responding to data protection breaches. This is to ensure that incidents are responded to promptly, risks are minimised, learning's identified and remedial actions are implemented.

This document has been designed to help and encourage all employees to achieve and maintain expected standards of conduct. It applies to all employees and anyone else working for the Company, and its aim is to ensure consistent and responsible practice.

This document does not form part of your Contractual Terms and Conditions of employment and the Company may at any time amend it without consultation or prior notice.
These procedures apply to all staff, suppliers, contractors, agency workers, volunteers, clients or anyone else who may handle or have an interest in personal data on behalf of the organisation.

PURPOSE

The purpose of an incident response is to ensure that:

- Data breach events are detected, reported, categorised and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of disclosure
- Mitigation improvements are made is put in place to prevent recurrence
- Serious breaches can be reported to the Information Commissioner
- Lessons learnt are communicated to the organisation as appropriate and can work to prevent future incidents.

DATA PROTECTION BREACHES

A data protection breach occurs when personal data (which includes any information that allows an individual to be identified), is processed without authorisation, and which may result in its security being compromised. For the purposes of this policy, data protection breaches include both confirmed and suspected breaches.

This procedure is concerned with the management of such data protection breaches, which involves the detection and reporting of breaches as well as learning from the breach and implementing appropriate remedial actions.
Most commonly, data protection breaches occur as a result of human error, theft, unauthorised access, equipment failure, hacking or loss
Examples of common incidents are

Type	Example	
Technical	Data Corruption Malware Corrupt Code Hacking	
Physical	Unescorted visitors in secure areas Break-ins to sites Thefts from secure sites Theft from unsecured vehicles/premises	Loss in transit/post Loss/ Misplacing memory stick/flash drive confidential papers left on public transport
Other	Data Input errors Non-secure disposal of hardware or paperwork Unauthorised disclosures (including verbal)	

When a data protection breach has been discovered, whatever the reason for the breach, the following procedure should be implemented.

DISCOVERY

All staff are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach or a potential breach has been discovered, where possible, a

Data Protection Breach Reporting & Procedure

Data Protection Breach Reporting Form should be completed to the fullest extent possible at that time, which provides full details concerning the breach or potential breach. This form should then be passed to one of

- **S** Sharon Young, Group Director, in my absence
- **W** William McVicar, Operations Director or
- **R** Roland Spella, Managing Director

as soon as possible and in any event within 2 hours of the discovery of the breach. If you need help completing the form, or are unable to complete the form, then any delay should be avoided and instead the matter should be reported immediately, either verbally or using electronic means, such as email.
Once a data protection breach has been reported, an initial assessment will be made concerning the content, quality of data involved and the potential impact and risk of the breach.
This is achieved by interviewing the key personnel involved in the breach and their line managers and collecting as much information as possible to determine how the breach occurred, what actions have been taken, whether outside agencies are involved and whether the data subjects have been notified
Not all data protection breaches will result in formal ICO Reporting action. Some will be false alarms or “near miss” events that do not cause immediate harm to individuals or the organisation. These should still be reported, as analysis of these instances will provide valuable process feedback and opportunity for continual improvement.

REPORTING

Following a discovery of a breach and the receipt of such a report, consideration will be made regarding whether the matter needs to be reported to the Information Commissioner’s Office (ICO) and whether individuals who are potentially affected need to be informed.
Current legislation states that any data protection breaches (irrespective of their severity) should be reported to the ICO as soon as possible and no later than 72 hours after their discovery, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.
In addition to this, the individuals affected by the breach should be informed if the breach is likely to pose a high risk to them. The individuals should be informed of the nature of the data breach and the steps that you are taking to protect their data. The incident should also be logged in the Data Protection Breach Register.

CONTAINMENT AND RECOVERY

As soon as possible after the discovery of an actual or suspected data protection breach, consideration should be given to: -

- **W** whether the breach has been contained as far as possible and whether any further steps can be taken to contain the data from further loss;
- **W** whether any steps can be taken to mitigate the impact and risk of the loss;
- **W** whether anything can be done to recover the data.

INVESTIGATION

Following the initial discovery/reporting of an incident, an investigation should be initiated to understand the full facts regarding the data protection breach. The extent of the investigation will be a matter for the Company to decide and may simply involve the collation of documents, or may be involve interviewing staff involved in the breach, collecting witness statements, etc.

REMEDIAL ACTIONS

Once the full facts have been ascertained, and the investigation has been concluded, consideration will be given to the learning’s from the breach and most importantly, what remedial actions the organisation needs to take to prevent a recurrence of the incident, this may include any appropriate disciplinary action for individuals implicated in the breach.
Actions should be documented on an action plan, which is reviewed on a regular basis thereafter to ensure that the actions have been carried out.
During and/or at the end of the completion of the investigation the Data Protection Breach Reporting Form and the Data Protection Breach Register will be updated to ensure that all the details of the events have been properly documented.
Any employees who act in breach of this policy or who do not implement it, may be subject to formal disciplinary proceedings, which may involve dismissal depending on the relevant circumstances.

Data Retention Policy

Policy Statement

This Company Policy and Procedure has been designed to help and encourage all employees to achieve and maintain expected standards of conduct. It applies to all employees and anyone else working for the Company, and its aim is to ensure consistent and fair practice and treatment.
This document does not form part of your Contractual Terms and Conditions of employment and the Company may at any time amend it without consultation or prior notice.

Purpose and Scope

HOT! is committed to managing and handling personal data in line with best practice and data protection principles. As such this Policy details the procedures to use to ensure timely and secure disposal of documents and records that are no longer required for business purposes.
The Company holds a wide variety of personal data, from *employees, workers, volunteers and contractors*, as well as *financial data, HR data, marketing data, client data and so on, many of which include personal data*. This data is held in various formats including*; letters, emails, contracts, forms, software systems* in both hard copy and electronic form.
It is essential that this policy is adhered to, as premature destruction of documents could result in an inability to defend claims, business difficulties and failure to comply with data protection legislation, whilst appropriate destruction and disposal will ensure that the storage space is maximised and we are not keeping documents for an unnecessarily long period of time which would breach data protection legislation.
This policy applies to all the information held by the Company and also any personal data that may be held by data processors (service providers) where they are processing information on the Company's behalf.
Everyone is responsible for ensuring that the records that they create/maintain are accurate, maintained and disposed of in accordance with this policy. It is recognised that the documentation created and maintained by the Company will change over time and therefore this policy should be viewed as a living document and it will be reviewed on an annual basis, or as necessary, if sooner.
This policy should be read in conjunction with the Data Protection Policy and the Data Protection Breach Reporting Policy.

Retention

Appendix 1 details the retention periods for specific types of documents and records.

Destruction/Disposal

Hard copies of confidential documents or personal data should be disposed of using the *[insert method e.g., confidential waste bins, shredder, etc.* Under no circumstances should any personal or confidential data be disposed of in any other manner, as this would potentially breach data protection legislation.
Disposal of documents which do not contain personal data or confidential information can be disposed of in any bin, or by recycling or by electronic deletion in the case of electronic documents.

Appendix 1 – Data Retention Periods

Business Function	**Examples of documents**	**Retention Period** (suggestions)
HR	Employee data, including all information on personnel files e.g. CVs, sickness information, holiday records, disciplinary information, training certificates etc (excluding those below)	5 years post-employment (NB 6 years in England)
	Maternity records	3 years after end of tax year in which maternity pay period ends
	References given after employment ends	5 years from date of reference
	Training records	Current year plus 2 years
	Probation/Appraisal/Performance management	Current year plus 5 years
	Data relating to ex-employee claims/threats/SAR	2 years after claim/SAR concluded, or 5 years post-employment whichever is later
	Parental Leave records	18 years from birth of child
	Pensioners records	12 years after benefit ceases
	Trust deeds and rules	Permanent
	Trustees' minutes	Permanent
	Candidate application forms/CVs and accompanying documentation (of applicants who aren't successful)	6 months post-date of recruitment decision
	Collective Agreements and accompanying documents	Permanent
	Disclosure Scotland data	6 months post-date of check
	Senior Executives' records	Permanent for historical purposes
Health & Safety	Reports on accidents at work or death	3 years from date of report
	Working Time Records	2 years
Payroll	PAYE records and records of hours worked for minimum wage purposes	6 years
Data Protection	Consents	6 years after the processing of data
Etc.	etc	etc

Employee Privacy Notice

To be issued to all existing employees and new employees prior to commencing employment

Data controller: HOT!

Named Person: Sharon Young

Contact details: 01475 717862

The company collects and processes personal data relating its employees to manage the employment relationship. The company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the company collect?

The company collects and processes a range of information about you. This includes:
your name, address and contact details, including email address and telephone number, date of birth and gender;
the terms and conditions of your employment;
details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the company;
information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
details of your bank account and national insurance number;
information about your [marital status, next of kin, dependants and emergency contacts];
information about your nationality and entitlement to work in the UK;
details of your schedule (days of work and working hours) and attendance at work;
details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
information about medical or health conditions, including whether or not you have a disability for which the company needs to make reasonable adjustments; and
The company may collect this information in a variety of ways. For example, data might be collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.
In some cases, the company may collect personal data about you from third parties, such as references supplied by former employers with your consent only.
Data will be stored in a range of different places, including in your personnel file, in the company's HR management systems and in other IT systems (including the company's email system).
*with your consent and when specified as part of the application/recruitment process

How is personal data collected?

We may collect this information in a variety of ways. For example, data might be collected through the CV with which you applied for employment; it may be obtained from your passport, ID card, driving licence or other identity documents you supply; it will also be obtained from forms you supplied or completed either at the point that you joined the company or during your employment. [This could include new starter forms, P45s from previous employers, HMRC starter checklists, MATB1 forms, paternity SC3 forms, self-certification sick forms, etc. Some information might also be obtained from correspondence with you; or through interviews and meetings.]

Where is the data held?

Data is held securely, including HR file locked in a restricted area accessible to senior management only, this is also stored electronically on the computer server with relevant restrictions for the purposes of confidentiality and is not accessible to any other staff member other than those authorised by Les Aikman.

Why does the company process personal data?

The company needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract,

to pay you in accordance with your employment contract and to administer benefits such as pension and any insurance entitlements.
In some cases, the company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.
In other cases, the company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the company to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the company complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees; and
- respond to and defend against legal claims.

Does the company process special categories of personal data?

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

- your trade union membership;
- your genetic or biometric data;
- your health;
- your sexual orientation;

We will only process special categories of your personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Sharon Young.
We do not need your consent to process special categories of your personal data when we are 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; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We might process special categories of your personal data for the purposes mentioned above 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; and

Employee Privacy Notice

To be issued to all existing employees and new employees prior to commencing employment

Who has access to data?

Your information may be shared internally, including with [members of the HR and Finance Team, including payroll, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles].

The company shares your data with third parties in order to [e.g. obtain pre-employment references from employers, obtain employment background checks from third-party providers. The company may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The company also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits such as pension etc, the provision of occupational health services and HR services.

How does the company protect data?

The company takes the security of your data seriously. The company has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the company keep data?

The company will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out in the Data Retention Policy.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the company to change incorrect or incomplete data;
- require the company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the company is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact Sharon Young.

If you believe that the company has not complied with your data protection rights, you can complain to the Information Commissioner.

What if I do not provide personal data?

You have some obligations under your employment contract to provide the company with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the company with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the company to enter a contract of employment with you. If you do not provide other information, this will hinder the company's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.