Group Data Protection Privacy Notice

For Staff & Job Applicants

Version	4	Effective	25 May 2018
Scheduled review date	This notice will be reviewed annually or as required		

The Company is committed to maintaining the accuracy, confidentiality and security of your personal information. This Privacy Notice describes the personal information that we collect from or about you, how we use it and to whom we disclose that information.

What Personal Information Do We Collect?
For the purposes of this Privacy Notice, personal information is any information about an identifiable individual. Personal information does not include anonymous or non-personal information.

We collect and maintain different types of personal information in respect of those individuals who seek to be, are, or were employed by us, including the personal information contained in:

- CVs and applications;
- references and interview notes;
- DBS and vetting information;
- Education and training information;
- Right to work information;
- Photographs, video and audio recordings including cctv imagery;
- letters of offer and acceptance of employment and other employment records;
- policy acknowledgement sign-off sheets;
- payroll information; including but not limited to national insurance number, banking and deposit information and national insurance number;
- wage and benefit information including annual leave information;
- forms relating to the application for welfare benefits;
- Health questionnaires and risk assessments including any medical condition or medication you are taking;
- beneficiary and emergency contact information;
- Disciplinary and grievance records;
- Your driving licence and insurance documentation; and
- Equal opportunities monitoring forms

In addition to the examples listed above, the personal information we collect includes information such as your name, home address, telephone, personal email address, date of birth, employee identification number, ethnicity, marital status, nationality, next of kin/emergency contact information, salary, biometric data provided and any other information necessary for business purposes, which is voluntarily disclosed in the course of an employee's application for and employment with us.

The above lists are non-exhaustive and applies across the Group. A complete list of information held on you is available from your Data Protection Officer (via your line manager).

As a general rule, we collect personal information directly from you. We may however also use recruitment consultants and recruitment websites to source potential applicants. In most

circumstances where the personal information that we collect about you is held by a third party, we will only process it in accordance with our legitimate interests, where necessary for the performance of our contracts or where obligated by law.

From time to time, we may use the services of third parties, such as recruitment agents and may also receive personal information collected by those third parties in the course of the performance of their services for us. In that case, we will take reasonable steps to ensure that such third parties have represented to us that they have the right to disclose your personal information to us.

Where permitted or required by applicable law or regulatory requirements, we may collect information about you without your knowledge or consent.

Why Do We Collect Personal Information?
The personal information collected is used and disclosed for our business purposes, including establishing, managing or terminating the employment relationship. It is necessary for the performance of our contract with you and/or performing our obligations under a contract as well as to meet our legal obligations and legitimate interests. Such uses include:

- determining eligibility and suitability for initial employment, including profiling from any previous job application to us, right to work checks and the verification of references and qualifications;
- administering pay and benefits including holiday pay;
- processing employee work-related claims (e.g. insurance claims, etc.)
- establishing training and/or development requirements;
- conducting performance reviews and determining performance requirements;
- assessing qualifications and suitability for a particular job, task, bonus or promotion;
- gathering evidence further to the disciplinary, grievance or whistleblowing procedure;
- establishing a contact point in the event of an emergency (such as next of kin);
- considering, assessing and preventing inequality or health & safety incidents or risks;
- complying with all regulatory and legislative requirements;
- compiling contact lists for internal purposes only;
- analysing workforce trends e.g. impact of Brexit or other regulatory or legislative changes;
- ensuring your security and the security of company held information and data; and
- such other purposes as are reasonably required by us for the performance of your contract; to protect vital interests; for the performance of a task in the public interest; to comply with our legal obligations; in accordance with our legitimate business interests or for the purpose of assessing your working capacity.

Monitoring
The work output of staff, whether in paper record, computer files, or in any other storage format belongs to us, and that work output, and the tools used to generate that work output, are always subject to review and monitoring by us.

In the course of conducting our business, we may monitor employee activities, attendance and our premises and property. For example, some of our locations are equipped with fingerprint log-in technology, tracking systems as you touch in and out of service users' homes and/or CCTV. Where in use, CCTV cameras are there for the protection of employees and third parties, and to protect against theft, vandalism and damage to our goods and property. Generally, recorded images are routinely destroyed and not shared with third parties unless there is suspicion of a crime, in which case they may be turned over to the police or other appropriate government agency or authority. Staff are referred to our CCTV Policy for further information. Pursuant to our Monitoring of Business Communications Policy and Procedure

and our Computer, Email and Internet Usage Policy, we have the capability to monitor all employees' computer and e-mail use.

This section is not meant to suggest that all employees will in fact be monitored or their actions subject to constant surveillance. It is meant to bring to your attention the fact that such monitoring may occur and may result in the collection of personal information from employees (e.g. through their use of our resources). When using company equipment or resources employees should not have any expectation of privacy with respect to their use of such equipment or resources.

How Do We Use Your Personal Information?
We may use your personal information for the purposes described in this Policy, or for any additional purposes that we advise you of and where your consent is required by law we have obtained your consent in respect of the use or disclosure of your personal information.

We may use your personal information without your knowledge or consent where we are permitted or required by applicable law or regulatory requirements to do so.

When Do We Disclose Your Personal Information?
We may share your personal information with our employees, contractors, advisers or consultants and other parties who require such information to assist us with establishing, managing or terminating our employment relationship with you, including: professional advisers, parties that provide products or services to us or on our behalf and parties that collaborate with us in the provision of products or services to you.

Also, your personal information may be disclosed:
- as necessary for the performance of our contract with you
- as permitted or required by applicable law or regulatory requirements. In such a case, we will try to not disclose more personal information than is required under the circumstances;
- to comply with valid legal processes such as warrants or court orders;
- as part of our regular reporting activities to other members of the Group, i.e. if necessary for the performance of your contract, to comply with a legal obligation or as part of our legitimate business interests;
- to protect the rights and property of the company or others;
- during emergency situations or where necessary to protect the vital interests or safety of a person or group of persons;
- to assess your working capacity;
- if in substantial public interest;
- where the personal information is publicly available; or
- with your consent.

Notification and Consent
Privacy laws do not generally require us to obtain your consent for the collection, use or disclosure of personal information for the purpose of establishing, managing or terminating the employment relationship. In addition, we may collect, use or disclose your personal information without your knowledge or consent where we are permitted or required by applicable law or regulatory requirements to do so.

Where your consent was obtained or required for our collection, use or disclosure of your personal information, you may, at any time, subject to legal or contractual restrictions and reasonable notice, withdraw your consent. All communications with respect to such withdrawal or variation of consent should be in writing and addressed to your Operations Manager for passing to the Data Protection Officer.

How is Your Personal Information Protected?

We endeavour to maintain physical, technical and procedural safeguards that are appropriate to the sensitivity of the personal information in question. This includes the use of firewalls and encryption as well as other information security requirements, systems and procedures. These safeguards are designed to protect your personal information from loss and unauthorised access, copying, use, modification or disclosure.

How Long is Your Personal Information Retained?
For unsuccessful job applicants or those who do not accept a position with us, we will generally destroy your data after 6 months unless you have requested that we retain it for longer.

For recruited staff, except as otherwise permitted or required by applicable law or regulatory requirements, we will only retain your personal information for as long as we believe it is necessary to fulfil the purposes for which the personal information was collected (including, for the purpose of meeting any contractual, legal, accounting or other reporting and regulatory requirements or obligations). We may, instead of destroying or erasing your personal information, make it anonymous such that it cannot be associated with or tracked back to you. In most cases your data will be deleted 6 years after you have left the company or as otherwise set out in accordance with our data retention schedule and/or as required by law.

Updating Your Personal Information
It is important that the information contained in our records is both accurate and current. If your personal information happens to change during the course of your employment, please keep us informed of such changes.

In some circumstances we may not agree with your request to change your personal information and will instead append an alternative text to the record in question.

Access to Your Personal Information
You can ask to see the personal information that we hold about you. If you want to review, verify or correct your personal information, please contact your Operations Manager. Please note that any such communication must be in writing.

When requesting access to your personal information, please note that we may request specific information from you to enable us to confirm your identity and right to access, and to assist us in searching for and provide you with the personal information that we hold about you. In specific circumstances, we may charge you a fee to access your personal information however we will advise you if this is the case and of any fee in advance.

Your right to access the personal information that we hold about you is not absolute. There are instances where applicable law or regulatory requirements allow or require us to refuse to provide some or all of the personal information that we hold about you. In addition, the personal information may have been destroyed, erased or made anonymous in accordance with our record retention obligations and practices.

If we cannot provide you with access to your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Your other legal rights
Data protection legislation also provides you with certain other rights. These are not always absolute rights and must be considered in the wider scope of the legislation. These rights are:

- right to erasure, also known as the right to be forgotten. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. In some circumstances this is not an absolute right;

- right to restrict processing. You have the right to ‘block’ or suppress processing of personal data. Again this is not an absolute right and will depend on the circumstances and any other legal/statutory obligations we may have;
- right to data portability – this is the right to have information provided in a structured, commonly used machine-readable format;
- right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- rights related to automated decision making including profiling.