Headline Data Protection Policy

General

This policy forms part of the company's suite of data protection policy. It is drafted so as to comply with the GDPR (General Data Protection Regulation) which comes into force in England on the 25th of May 2018 and which replaces the Data Protection Act 1998. This policy applies to all employees of the company.

In the event of any query about any aspect of the company's data protection regime, you should contact the Data Protection Officer.

The Data Protection Officer is *James Collinge*

Legal Framework

The Company holds and processes information about individuals. This means that the Company is a 'Data Controller' for the purposes of data protection legislation ("the Legislation"). Any breach of the Legislation could have serious legal consequences.

Failure to comply with this policy or to the other policies comprised in the company's data protection regime will be treated as a disciplinary matter.

Key Concepts

The Legislation relates to personal data. In broad terms, personal data is any information about living, identifiable individuals which is held by the company.

Personal data must be obtained only for specified, lawfully and transparent purposes and must not be processed in any way which is incompatible with those purposes. Processing data covers just about anything you can do with information, including collecting it, storing it, using it, passing it to third parties and destroying it.

The personal data that we keep must be accurate, must be limited to what is necessary for the purpose for which the data is being processed and must not be kept for any longer than is necessary. Personal data must also be kept secure.

Certain types of data are known as "special category data". Special category data is any data which would identify a living person and which relates to information about their:-

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where that information is used for ID purposes)
- Health
- Sex life

- Sexual orientation

Processing Data Lawfully

If the company wishes to process personal data, it must be able to demonstrate that at least one of the following six lawful bases for processing applies:-

- Consent (that the individual has agreed to the processing of their data for a specific purpose)
- Contract (the processing of the data is necessary pursuant to a contract the company has with the individual)
- Legal Obligation (the processing is necessary to satisfy a legal requirement)
- Legitimate Interests (that there is a good reason for processing the data which outweighs the potential impact on the individual)
- Vital Interests
- Public Tasks

The last two bases (vital interests and public tasks) are extremely unlikely to apply to anything which the company does and if you believe that you need to process data for either of these reasons, you should not do so without first clearing it with the DPO (or their substitute if the DPO is not available).

Every processing activity which the company carries out is covered by a Privacy Notice. The Privacy Notice confirms the lawful basis for processing and provides the individual whose data is being processed with requisite information about the processing activities and their rights.

Only the DPO and other employees who have been specifically authorised by the company may complete or issue Privacy Notices.

If you have been authorised to prepare a Privacy Notice, you should refer to the **Data Protection Policy – Writing Privacy Notices** together with the accompanying notes. These documents all form part of the company's suite of data protection policies.

In the event that a company is processing special category data, then in addition to identifying a lawful basis for processing (from the list set out above), we must also be able to satisfy one of the following additional criteria:-

- The data subject has given explicit consent
- Employment/social security/social protection
- Data has been made public by data subject
- The processing is necessary for a legal claim
- The processing is necessary to assess the working capacity of an employee
- The processing is necessary in the vital interests of the data subject
- Legitimate activities of political /philosophical/religious or trade union body

- The processing is in the substantial public interest
- Processing is in the public interest in the area of public health
- The processing is necessary for archiving purposes

Again, it is only those employees who are authorised to prepare Privacy Notices who are entitled to decide which (if any) of these additional criteria apply to an act of processing.

Data about Criminal Offences

There are further restrictions when it comes to processing data regarding an individual's history of criminal offending. If, for any reason, you need to process such data, you should not do so without first seeking authority from the DPO. In the general run of events, it is extremely unlikely that any such authority could be given due to the specific protections afforded to criminal offence data by the Legislation.

Security and Non-disclosure

All employees are responsible for making sure that any personal data that the company holds (or which you use in the course of your employment or which you notice in the course of your employment) is kept securely and is not disclosed, either orally or in writing, to any third party other than pursuant to the provisions of a Privacy Notice. You should be especially wary of accidentally disclosing personal data.

To ensure that data is adequately protected, the company has a data security policy which forms part of the company's suite of data protection policies. You should be familiar with this policy.

At a very basic level, desks should be kept clear of paper documents containing personal data unless those documents are actively being worked upon. Manual records containing personal data should always be kept secure, for example in a locked and fireproof filing cabinet.

Much of the personal data which the company handles is kept electronically. You should ensure that all computer files and applications are closed when you have finished working on them, that computers are shut down when you have finished work (and not just left on standby) and that you only access those computers for which you have specific permission. Computers should be password protected and as well as being switched off when you finish work, should be switched off when they are to be left unattended. Your password should not be written down or shared with others and if you fear that your password had been disclosed to third parties or the security of your computer has been compromised, you should notify your line manager or the DPO as soon as possible.

Online scams are increasingly commonplace and increasingly sophisticated. You should not open links or attachments in e-mails which do not come from trusted sources. Wherever possible, you should check the address of incoming e-mails and the return address as specified in any e-mails as these will often give away the fact that a particular e-mail is not genuine or from who it purports to be.

If you accidentally open a link or an attachment attached to a message, you should notify your line manager or DPO immediately.

If you become aware that messages have been sent to third parties using your e-mail address or the e-mail addresses of your colleagues, you should notify your line manager or the DPO.

Early notification of issues is important to ensure that we maintain data security and abide by our breach reporting requirements.

You must not remove personal data (or indeed any confidential, company information) from the workplace without the express permission of the company. If you receive the necessary permission, you must ensure that all information in your possession is kept safe at all times and is not left unattended in any vehicle or public place. Where you keep information at home, you should take all such steps as are reasonably practicable to protect the integrity of the information, including keeping it away from the eyes of third parties (including family members) and, wherever possible, ensuring that the information is not left unattended.

If any personal data is disclosed or destroyed by mistake, you should report it immediately to the DPO.

The Rights of Data Subjects

Individuals have certain rights in relation to data which the company holds about them. The company must notify individuals of the information held about them and this is done through the Privacy Notice system.

As an employee of the company, some of your personal data will be processed for purposes permitted by the Legislation. You have the same rights as would apply to third party individuals whose data the company processes.

The rights of data subjects are set out in more detail in the Data Protection – Individual Rights Policy.

Specifically, individuals have the right of access to data held about them. Again, this right extends to you as an employee of the company.

Data subjects have the right to obtain the following:-

- Confirmation that their data has been processed
- Access to their personal data
- Other relevant information (which will normally be included in Privacy Notices)

Any request for disclosure of data held about a data subject is known as a "subject access request". Companies are no longer allowed to make any charge for complying with a subject access request although we can still charge a reasonable fee where a subject access request is manifestly unfounded or excessive, particularly when such requests have been made on more than one occasion. A fee may also be charged for provision of information which has already been provided. Any fees charged must be limited to the reasonable cost of providing the information.

Information must be provided without delay and in any event within one month of the subject access request. Where a subject access request is complicated or where there is more than one request, the deadline for complying with the request may be extended by up to two months.

Breach Reporting

All employees are subject to the company's Breach Reporting Policy which can be found at **Data Protection – Breach Reporting Policy**. Please familiarise yourself with the provisions of this policy.

Employment Records

As your employer, we hold and use personal information relating to all employees. Some of the information that we process could be classified as 'sensitive personal data'. This would include information relating to membership of a trade union, your health, any criminal convictions or offences.

Most of the information we hold about you will come directly from you. However, it may be necessary for us to collect information from other sources, such as previous employers (for example, to obtain a reference or to assess eligibility for parental leave). We may also hold information regarding medical conditions, pursuant to the Sickness and Sick Absence policy.

The information held about you will normally be held on the lawful bases of Legal Obligation (for example, we have to hold certain personal data so that we can process tax and national insurance payments to HMRC), Contract (as we have a contract of employment with you and many of our other policies and procedures have contractual effect) or Legitimate Interests (for example, to allow us to hold data for the purposes of equal opportunities monitoring).

Privacy Notices in relation to each of the bases for processing your personal data can be obtained direct from the DPO Officer James Collinge