1. DATA PROTECTION POLICY

Policy statement

1.1 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff and we recognise the need to treat it in an appropriate and lawful manner.

1.2 The types of information that we may be required to handle include details of current, past and prospective employees, contractors, suppliers, clients and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 and the General Data Protection Regulation EU 2016/679 as updated and amended from time to time (the Data Protection Legislation). The Data Protection Legislation imposes restrictions on how we may use that information. There are also further restrictions contained in the Privacy and Electronic Communications Regulations 2003 and the E-Privacy Directive 2002/58/EC.

1.3 Any breach of this policy will be taken seriously and may result in disciplinary action.

Status of the policy

1.4 This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

1.5 The Data Protection Co-ordinator is responsible for ensuring compliance with the Data Protection Legislation and with this policy on behalf of the Managing Director. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Co-ordinator.

1.6 If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with your line manager or the Data Protection Co-ordinator immediately as we have a legal duty to report any Data Protection Legislation breaches.

Definition of data protection terms

1.7 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

1.8 **Data Subjects for** the purpose of this policy include all living individuals about whom we hold personal data. All Data Subjects who are in the European Union are entitled to these protections regardless of where we are based. All Data Subjects have legal rights in relation to their personal data.

1.9 **Personal Data** means data relating to a living individual who can be identified from that data (or from that data and other information which we have access to). Personal Data can be factual (such as a name, address or date of birth, online identifier) or it can be an opinion (such as a performance appraisal).

1.10 **Data Controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is processed, whether alone or jointly with another. They have a responsibility to establish practices and policies in line with the Data Protection Legislation. We are the Data Controller of all Personal Data used in our business.

1.11 **Data Users** include employees or contractors whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies at all times.

1.12 **Data Processors** include any person who processes Personal Data on behalf of a Data Controller. Employees of Data Controllers are excluded from this definition but it could include suppliers which handle Personal Data on our behalf. Data Processors have additional obligations to Data Controllers under the Data Protection Legislation which they must comply with.

1.13 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

1.14 **Sensitive Personal Data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, genetic data, biometric data, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive Personal Data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

Data protection principles

1.15 Anyone processing Personal Data must comply with the principles of the Data Protection Legislation. The Personal Data of Data Subjects must be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(d) accurate and, where necessary, kept up to date;

(e) kept for no longer than is necessary for the purposes for which it is processed; and

(f) processed in a way that is appropriately secure, including protecting it against unauthorised or unlawful processing, accidental loss, destruction or damage.

1.16 Personal Data must always be processed in accordance with the Data Subject's rights and must not be transferred to a country outside of the European Union unless that country's data protection standards have been recognised as being adequate.

Fair and lawful processing

1.17 The Data Protection Legislation is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the Company), who the Data Controller's representative is (in this case the Data Protection Co-ordinator), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

1.18 For Personal Data to be processed lawfully, certain conditions have to be met. This may include requirements that the Data Subject has consented to the processing, or that the processing is necessary for a particular reason such as our legal obligations or performance of a contract which the Data Subject is a party to. Sensitive Personal Data cannot be processed unless the Data Subject has given explicit consent or the processing is otherwise permitted by the Data Protection Legislation.

Processing for limited purposes

1.19 Personal Data may only be processed for the specific purposes notified to the Data Subject when the data was first collected or for any other purposes specifically permitted by the Data Protection Legislation. This means that Personal Data must not be collected for one purpose and then used for another unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

Adequate, relevant and non-excessive processing

1.20 Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate data

1.21 Personal Data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Timely processing

1.22 Personal Data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

Processing in line with Data Subject's rights

1.23 Data must be processed in line with Data Subjects' rights. Data Subjects have a right to:

(a) be informed of their rights and how their data will be processed;

(b) request access to any data held about them by a Data Controller;

(c) prevent the processing of their data for direct-marketing purposes;

(d) ask to have inaccurate data amended;

(e) request to have all of their data deleted (the right to be forgotten);

(f) object to their data being processed for particular reasons including profiling; and

(g) request that their data is transferred to another Data Controller.

Data security

1.24 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss and we may incur large fines if we are in breach of the Data Protection Legislation.

1.25 The Data Protection Legislation requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data may only be transferred to a third-party Data Processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself. We may only transfer data to a country outside of the European Union where they have been recognised as having adequate protections in place.

1.26 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) "Confidentiality" means that only people who are authorised to use the data can access it;

(b) "Integrity" means that Personal Data should be accurate and suitable for the purpose for which it is processed; and

(c) "Availability" means that authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored in a way which means that it is only accessible by those who need access to it.

1.27 Security procedures include:

(a) Encryption: Ensuring that all Personal Data which we process is encrypted.

(b) Data Backup: All Personal Data must be backed up so that if data is destroyed accidentally it can be restored.

(c) Entry Controls: Any stranger seen in entry-controlled areas should be reported.

(d) Secure Lockable Desks and Cupboards: Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.

(e) Methods of Disposal: Paper documents should be shredded. Any electronic equipment capable of storing Personal Data should be securely wiped and disposed of appropriately.

(f) Equipment: Data Users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Monitoring

1.28 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our

role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be monitored.

1.29 We may retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing; or

(d) to comply with any legal obligation.

Dealing with requests for information

1.30 A formal request from a Data Subject for information that we hold about them must be made in writing. If you receive a written request you should forward it to the Data Protection Co-ordinator immediately.

Providing information over the telephone

1.31 Any person dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

(a) check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

(c) refer to the Data Protection Co-ordinator for assistance in difficult situations. No-one should be bullied into disclosing personal information.