DATA PROTECTION POLICY

1. INTRODUCTION

1.1 This policy is intended to meet the requirements of the Data Protection Act 2018 (the 2018 Act) and the EU General Data Protection Regulation (GDPR) and comply with our legal obligations in respect of data privacy and security under the 2018 Act and the GDPR.

1.2 This policy is divided into three parts: Part 1 containing the Principal Policy, Part 2 containing the Data Retention Policy and Part 3 containing the Data Security Policy.

1.3 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.

1.4 The Company has appointed Rachel Bennett (Recruitment Co-Ordinator) as the person with responsibility for data protection compliance within the Company. They should be contacted at concerning questions or requests for further information, about this policy.

1.5 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.

1.6 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.

PART 1 - PRINCIPAL DATA PROTECTION POLICY

2. PURPOSE AND SCOPE

2.1 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 have a duty to notify you of the information contained in this policy.

2.2 This policy applies to current and former employees, workers, volunteers, apprentices, consultants and job applicants. 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.

2.3 The Company has separate policies and privacy notices in place in respect of customers, suppliers and other categories of data subject. A copy of these can be obtained from the person responsible for data protection compliance (Rachel Bennett).

2.4 The Company will hold data for specified periods of time appropriate to the type of data. These periods of time are contained in Part 2 of this policy in the Data Retention Policy. We will only hold data for as long as necessary for the purposes for which we collected it.

2.5 The Company has measures in place to protect the security of your data in accordance with our Data Security Policy. These security measures are contained in Part 3 of this policy.

3. DATA PROTECTION PRINCIPLES

3.1 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.
- Be processed securely.

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

4. DEFINING PERSONAL DATA

4.1 '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.

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

4.3 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.

4.4 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.
- Absence records.
- 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).
- Information about your termination of employment (or services) including resignation, dismissal and redundancy letters, minutes of meetings, settlement agreements and other related correspondence.
- Any other category of personal data which we may notify you of from time to time.

5. DEFINING SPECIAL CATEGORIES OF PERSONAL DATA

5.1 '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 sex life and sexual orientation.
- Any criminal convictions and offences.

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

6. DEFINING PROCESSING

6.1 '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.
- Restriction, destruction or erasure.

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

7. DATA SECURITY

The Company takes the security of HR-related personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. A Data Security Policy is contained in Part 3 of this Data Protection Policy.

Where the Company engages third-parties to process personal data on its behalf, such parties 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.

8. HOW PERSONAL DATA WILL BE PROCESSED

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

8.2 We will use your personal data on a lawful basis for:

- Contractual - performing the contract of employment (or services) between us.
- Legal Obligation – complying with any legal obligation.
- Legitimate Interest - 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 Clause 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.

9. REASONS FOR PROCESSING PERSONAL DATA

9.1 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).
For example, in the following circumstances:

- 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.
- To decide whether to promote you.
- To carry out a disciplinary or grievance investigation or procedure in relation to you or someone else.
- To monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others.
- Paying tax and national insurance.
- To provide a reference upon request from another employer.
- Running our business and planning for the future.
- The prevention and detection of fraud or other criminal offences.

9.2 We might process special categories of your personal data specifically for the following purposes:

- Training you and reviewing your performance.
- To decide whether and how to manage your performance, absence or conduct.
- 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 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.
- 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 and other laws which affect us.
- To answer questions from insurers in respect of any insurance policies which relate to you.
- To defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure.
- For any other reason which we may notify you of from time to time.

9.3 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 Rachel Bennett.

9.4 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.
- Where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

9.5 We might process special categories of your personal data for the purposes in sub- clause 9.2 above. In particular, we will use information in relation to:

- Your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities.
- Whether you have a disability which the company needs to make reasonable adjustments.
- 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.

- Your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

9.6 Automated decision-making

We do not take automated decisions about you using your personal data or use profiling in relation to you or your employment. However, you will be notified if this position changes.

10. SHARING PERSONAL DATA

10.1 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.

10.2 The Company also shares your data with third-parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services. It also shares your data with outsourced Employment Law and HR services to ensure compliance with Employment legislation.

10.3 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.

10.4 Transfer of Data outside the European Economic Area

The Company will not transfer your data to Countries 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.

11. PROCESSING PERSONAL DATA FOR THE COMPANY BY YOU

11.1 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.

11.2 The person named in sub-clause 1.4 of this policy 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.

11.3 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.

11.4 You should not share personal data informally.

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

11.6 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.

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

11.8 You should use strong passwords.

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

11.10 Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.

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

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

11.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the person responsible for data protection compliance (Rachel Bennett).

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

11.15 You should not take personal data away from Company's premises without authorisation from your Line Manager.

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

11.17 You should ask for help from the person responsible for data protection compliance (Rachel Bennett) if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

11.18 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.

11.19 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.

12. DATA BREACHES

12.1 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.

12.2 If you are aware of a data breach you must contact Rachel Bennett immediately and keep any evidence you have in relation to the breach.

13. SUBJECT ACCESS REQUESTS

13.1 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 person responsible for data protection compliance (Rachel Bennett) who will coordinate a response.

13.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to Rachel Bennett. 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.

13.3 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.

14. DATA SUBJECT RIGHTS

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

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

14.3 You can correct any inaccuracies in your personal data. To do this you should contact Rachel Bennett.

14.4 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 Rachel Bennett.

14.5 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 Rachel Bennett.

14.6 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.

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

14.8 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.

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

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

14.11 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 Rachel Bennett.

14.12 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.

PART 2 - DATA RETENTION POLICY

15. INTRODUCTION

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The Company will therefore:

- Review the length of time its keeps personal data.
- Consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it.
- Securely delete information that is no longer needed for this purpose or these purposes.
- Update, archive or securely delete information if it goes out of date.

16. DELETING DATA

Discarding data too soon would be likely to disadvantage the Company and quite possibly, inconvenience the people the information is about as well.

Personal data will be regularly reviewed and anything no longer needed will be deleted. Information that does not need to be accessed regularly, but which still needs to be retained, will be safely archived or put offline.

In retaining data, the Company will take account of any professional rules or regulatory requirements that apply. The retention periods will be regularly reviewed to consider whether it is being held too long or conversely if it is being deleted prematurely. However, if any records are not being used, consideration will be given to whether they need be retained.

17. PERSONAL DATA AT THE END OF ITS RETENTION PERIOD

At the end of the retention period, or the life of a particular record, it will be reviewed and deleted, unless there is some special reason for keeping it.

Where appropriate a record may not be permanently deleted and it may be archived instead. If a record is archived or stored offline, this will reduce its availability and the risk of misuse or mistake. However, a record will only be archived (rather than deleted) if it is considered essential to retain it. In order to comply with data protection principles subject access to it will still be permissible. If a record is deleted from a from a live system, it will also be deleted from any back-up of the information on that system.

18. DATA RETENTION PERIODS

We will only hold data for as long as necessary for the purposes for which we collected it and will hold data for specified periods of time appropriate to the type of data.

18.1 Statutory Retention Periods

The main UK legislation regulating statutory retention periods is summarised below. If the Company is in doubt, it will retain records for at least 6 years (5 in Scotland), to cover the time limit for bringing any civil legal action.

Record types:

- Accident books, accident records/reports
  Statutory retention period: **3 years from the date of the last entry** (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos).
  Statutory authority: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).

- Accounting records
  Statutory retention period: **3 years for private Companies**, 6 years for public limited companies.
  Statutory authority: Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.

- Income tax and NI returns, income tax records and correspondence with HMRC
  Statutory retention period: **not less than 3 years after the end of the financial year** to which they relate.
  Statutory authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).

- Medical records and details of biological tests under the Control of Lead at Work Regulations
  Statutory retention period: **40 years from the date of the last entry**.
  Statutory authority: The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676).

- Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)
  Statutory retention period: **40 years from the date of the last entry**.
  Statutory authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).

- Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos and medical examination certificates
  Statutory retention period: **(medical records) 40 years from the date of the last entry; (medical examination certificates) 4 years from the date of issue**.
  Statutory authority: The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632).

- Medical records under the Ionising Radiations Regulations 1999
  Statutory retention period: until the person reaches 75 years of age, but in any event for at least **50 years**.
  Statutory authority: The Ionising Radiations Regulations 1999 (SI 1999/3232).

- Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)
  Statutory retention period: **5 years from the date on which the tests were carried out**.
  Statutory authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).

- Records relating to children and young adults
  Statutory retention period: **until the child/young adult reaches the age of 21**.
  Statutory authority: Limitation Act 1980.
- Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity
  Statutory retention period: **6 years from the end of the scheme year in which the event took place**.
  Statutory authority: The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103).

- Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence
  Statutory retention period: **3 years after the end of the tax year in which the maternity period ends**.
  Statutory authority: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.

- Wage/salary records (also overtime, bonuses, expenses) Statutory retention period: **6 years**.
  Statutory authority: Taxes Management Act 1970.

- National minimum wage records
  Statutory retention period: **3 years after the end of the pay reference period** following the one that the records cover.
  Statutory authority: National Minimum Wage Act 1998.

- Records relating to working time
  Statutory retention period: **2 years from date on which they were made**.
  Statutory authority: The Working Time Regulations 1998 (SI 1998/1833).

18.2 Recommended (Non-Statutory) Retention Periods

For many types of HR records, there is no definitive retention period, therefore it is up to the Company to decide how long to keep them. The Company has therefore considered the necessary retention period for them, depending on the type of record.

The retention periods listed below is based on the time limits for potential UK tribunal or civil claims.
The UK Limitation Act 1980 contains a 6-year time limit for starting many legal proceedings. So, where documents may be relevant to a contractual claim, the Company will retain them for at least a corresponding 6-year period.

Record types:

- Actuarial valuation reports
  Recommended retention period: **permanently**.

- Application forms and interview notes (for unsuccessful candidates)
  Recommended retention period: **6 months to a year**. (Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicant’s documents will be transferred to the personnel file in any event.
- Assessments under health and safety regulations and records of consultations with safety representatives and committees
  Recommended retention period: **permanently**.

- Inland Revenue/HMRC approvals
  Recommended retention period: **permanently**.

- Money purchase details
  Recommended retention period: **6 years after transfer or value taken**.

- Parental leave
  Recommended retention period: **5 years from birth/adoption** of the child or 18 years if the child receives a disability allowance.

- Pension scheme investment policies
  Recommended retention period: **12 years from the ending of any benefit payable** under the policy.

- Pensioners' records
  Recommended retention period: **12 years after benefit ceases**.

- Personnel files and training records (including disciplinary records and working time records)
  Recommended retention period: **6 years after employment ceases**.

- Redundancy details, calculations of payments, refunds, notification to the Secretary of State
  Recommended retention period: **6 years from the date of redundancy**.

- Senior executives' records (that is, those on a senior management team or their equivalents)
  Recommended retention period: **permanently** for historical purposes.

- Statutory Sick Pay records, calculations,
  certificates, self-certificates Recommended retention period: The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) abolished the former obligation on employers to keep these records. Although there is no longer a specific statutory retention period, employers still have to keep sickness records to best suit their business needs. It is advisable to keep records for at least 3 months after the end of the period of sick leave in case of a disability discrimination claim. However, if there were to be a contractual claim for breach of an employment contract it may be safer to keep records for **6 years after the employment ceases**.

- Time cards
  Recommended retention period: **2 years after audit**.

- Trade union agreements
  Recommended retention period: **10 years after ceasing to be effective**.

- Trust deeds and rules
  Recommended retention period: **permanently**.
- Trustees' minute books
  Recommended retention period: **permanently**.

- Works council minutes
  Recommended retention period: **permanently**.

PART 3 - DATA SECURITY POLICY

19. INTRODUCTION

This policy outlines behaviours expected of employees when dealing with data and provides a classification of the types of data with which they should be concerned.

19.1 Purpose

As an employee of the Company if you have access to data then must protect personal, restricted, confidential and sensitive data and ensure it is processed in accordance with the data protection principles contained in the Principal Data Protection Policy and further detailed below.

19.2 Scope

Any employee, contractor or individual with access to Company systems and personal data. The definition of data to be protected is defined as all data that is described in Part 1 of this policy, ie. Principal Data Protection Policy.

20. DATA PROTECTION PRINCIPLES

The following is in addition to the Data Protection Principles stated in Clause 3 of the Principal Data Protection Policy (Part 1).

20.1 Staff whose work involves using and or processing data subjects described in clause 2.2 of Part 1 Principal Data Protection Policy must comply with this policy and with the eight legal data protection principles which require that personal information is:

a) Processed fairly and lawfully. We must always have a lawful basis to process personal information. In most (but not all) cases, the person to whom the information relates (the Subject) must have given consent. The Subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed.

b) Processed for limited purposes and in an appropriate way. Personal information must not be collected for one purpose and then used for another. If we want to change the way we use personal information we must first tell the Subject.

c) Adequate, relevant and not excessive for the purpose.

d) Accurate. Regular checks must be made to correct or destroy inaccurate information.

e) Not kept longer than necessary for the purpose. Information must be destroyed or deleted when we no longer need it. For guidance on how long

particular

information should be kept, contact the Data Controllers representative.

f) Processed in line with Subjects' rights. Subjects have a right to request access to their personal information, prevent their personal information being used for direct-marketing, request the correction of inaccurate data and to prevent their personal information being used in a way likely to cause them or another person damage or distress.

g) Secure. See further information about data security below.

h) Not transferred to people or organisations situated in countries without adequate protection.

20.2 Some personal information needs even more careful handling. This includes information about a person's racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, genetic or biometric data, health, sex life and sexual orientation; and any criminal convictions and offences.

21. EMPLOYEE REQUIREMENTS

21.1 You must protect personal information in Company possession from being accessed, lost, deleted or damaged unlawfully or without proper authorisation through the use of data security measures.

21.2 Maintaining data security means making sure that:

a) Only staff who are authorised to use the information can access it.

b) Information is accurate and suitable for the purpose for which it is processed.

c) Authorised persons can access information if they need it for authorised purposes.

Personal information therefore should not be stored on individual computers but instead on our central system.

21.3 The Company by law, must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

21.4 Personal information must not be transferred to any person to process, eg. while performing services for us on or our behalf, unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

21.5 Security procedures include:

a) Physically securing information. Any desk or cupboard containing confidential information must be kept locked. Computers should be locked with a password or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
b) Controlling access to premises. Staff should report to security if they see any person they do not recognised in an entry-controlled area.

21.6 Telephone Precautions. Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

a) The identity of any telephone caller must be verified before any personal information is disclosed.

b) If the callers identity cannot be verified satisfactorily then they should be asked to put their query in writing.

c) Do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the Data Controllers representative.

21.7 Methods of disposal – Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CD's or memory sticks or similar must be rendered permanently unreadable.