1. Policy Statement

1.1 Data Protection Legislation dates back to 1984. When the first Data Protection Act (DPA) came into the UK, it was introduced to protect the public from the misuse of personal computerised information held on any individual and to allow access to that information held by any organisation keeping computer records.

1.2 The Data Protection Act 1998 enhanced and broadened the scope of the 1984 Act. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge or consent.

1.3 Everyone has rights with regard to how their personal information, which may be held on paper or on a computer or other media, is handled. The information is subject to certain legal safeguards specified under the DPA and other regulations about how we retain and use this information.

2. Scope

2.1 This policy sets out the Company rules and guidelines on data protection and the legal conditions for obtaining; handling; processing; storing; transferring and destroying personal information.

2.2 This policy gives details about the type of information that the Company keeps and the purpose for retaining that information.

2.3 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

3. Responsibilities

3.1 The board has overall responsibility for the effective operation of this policy and for ensuring compliance with data protection law.

3.2 HR is responsible for ensuring that employees with responsibility for handling personal data receive adequate training and guidance.

3.3 The Compliance Manager is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues.

3.4 The HR Manager is responsible for ensuring employee records are maintained in accordance with data protection law.

3.5 Directors, managers and all those in supervisory positions are responsible for developing and encouraging good information handling practices within the Company.

3.6 Managers have a responsibility to ensure that information they process or are privy to, is handled in accordance with the principles of this policy.

3.7 Compliance with data protection legislation is the responsibility of all members of the Company.

3.8 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 the relevant person stated in this section.

4. Associated documents

The following documents are relevant to this policy:

- Information and Communications Policy

5. General principles

5.1 The types of information that we may be required to handle include details of current, past and prospective employees, clients, suppliers, customers and others that we communicate with and we recognise the need to treat it in an appropriate and lawful manner.

5.2 Throughout employment and for as long a period as is necessary following the termination of employment, the Company will need to keep information for purposes connected with an employee's employment.

5.3 All employee related data held will be for our management and administrative use only, but from time to time we may need to disclose some information we hold about employees to relevant third parties.

5.4 We may also transfer information to another Group or Organisation, solely for purposes connected with an employee's career or the management of the Company's business.

6. Definitions of data protection terms

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

6.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

6.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

6.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

6.5 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and information security policies at all times.

6.6 **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.

6.7 **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.

6.8 **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, 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. See also paragraph 8 below.

(a) The Company also consider that sensitive personal data shall also include:

(i) Information relating to the Company;

(ii) Information relating to the Company's products and/or services;

(iii) Information relating to the Company's customers; and

(iv) Information relating to the Company's suppliers.

6.9 **A 'relevant filing system'** is "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".

7. Data protection principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully;

(b) Obtained for one or more specified and lawful purpose(s) and only further processed in a manner compatible with that purpose(s);

(c) Adequate, relevant and not excessive in relation to the purpose(s) for which this processing is to take place;

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

(e) Not kept longer than necessary for the purpose(s) it was obtained;

(f) Processed in line with data subjects' rights;

(g) Secure, with appropriate technical and procedural measures to protect against unauthorised or unlawful processing and accidental loss or destruction; and

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

8. Fair and lawful processing

8.1 All processing of personal data must be “fair and lawful” and must not adversely affect the rights of the data subject.

8.2 The data subject must be told:

(a) The identity of the data controller: BCM Construction Limited;

(b) Who their representative is: The Compliance Manager;

(c) The purpose for which the data is to be processed; and

(d) The identity of anyone to whom the data may be disclosed and/or transferred.

8.3 Additional conditions apply to the processing of personal data. These include, among other things:

(a) The data subject must have consented to the processing of their data.

(b) The processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed.

(c) That 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 Act. This means that personal data must not be collected for one purpose and then used for another. 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.

(d) When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

9. Employee data

9.1 The following information relating to past, current and prospective employees may be obtained and processed by the Company:

(a) Information gathered about an employee and any references obtained during recruitment;

(b) Details of terms of employment;

(c) Payroll, tax and National Insurance information;

(d) Performance information;

(e) Details of position and job duties;

(f) Health records;

(g) Absence records, including holidays and self-certification forms;

(h) Details of any disciplinary investigations and proceedings;

(i) Training records;

(j) Contact name and addresses;

(k) Correspondence with the Company and other information provided to the Company.

9.2 The following information may also be held for which disclosure to any person will be made only when strictly necessary for the purposes set out below:

(a) An employee's health, for the purposes of:

(i) Compliance with our health and safety and our occupational health obligations;

(ii) HR administration, for example to consider how an employee's health affects his or her ability to do his or her job; and

(iii) To assess the need for reasonable adjustments to be made to assist an employee with a disability.

(b) Unspent convictions to enable us to assess an individual's suitability for employment;

(c) Employees' salary and benefit details for the administration of insurance, pension, sick pay and any other related benefits.

9.3 Employees must notify their line manager or the HR Manager when their personal data changes, e.g. address, bank details, marital status, telephone number etc.

9.4 If a Manager is to keep any record containing personal data on any employee, either on computer or in manual form, they must ensure that the HR department has a copy.

10. Accurate and timely processing

10.1 Personal data must be accurate and kept up to date and accordingly, all such data held by the Company will be reviewed periodically to ensure compliance.

10.2 Steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

10.3 Inaccurate or out-of-date data will be destroyed.

10.4 Personal data will not be kept longer than is necessary and will be destroyed or erased from our systems when it is no longer required.

(a) Employees pay and personnel records (excluding pension documentation) will be deleted from the Company's computers or destroyed (if manually recorded) at the end of the seventh year following the year in which the employee leaves the Company.

11. Data subject's rights

Data subjects have a right to:

(a) Request access to any data held about them by a data controller; see paragraph 14.

(b) Prevent the processing of their data for direct-marketing purposes;

(c) Ask to have inaccurate data amended;

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. Data Security

12.1 All personal and sensitive personal data must be protected against unlawful or unauthorised processing and accidental loss or damage.

12.2 The Act 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.

12.3 Personal data may only be transferred to a third-party data processor that agrees to comply with those procedures and policies, or puts in place adequate measures.

12.4 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.

(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 on our central computer system instead of individual PCs.

12.5 The Company's security procedures include:

(a) Entry controls - Any stranger seen in entry-controlled areas should be reported.

(b) 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.

(c) Access to computer screens or manual records holding employees' information restricted to authorised personnel.

(d) 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.

(e) Disposal - Paper documents should be securely shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

13. Data Transfer

13.1 Authorisation must be sought from the Compliance Manager prior to the transfer of any sensitive or confidential data.

13.2 The sender and recipient of personal data must enter into a written contract in which the recipient undertakes to keep the personal data confidential and to ensure that it is protected whilst in the recipient's hands.

13.3 All sensitive and confidential information should be encrypted, compressed and password protected before transmission. If you do not know how to do this you should seek appropriate assistance from the IT department.

13.4 If data is to be transferred through memory sticks, CD-ROMs or similar formats then the secure handling of these devices must be ensured. No such device should be sent through the open post. A secure courier service must always be used and the recipient should be clearly stated.

13.5 If data is sent via a courier the intended recipient must be made aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received and liaising with the courier service if there is any delay in the receipt of the data.

14. Dealing with subject access requests

14.1 You have a right to request information that we hold about you. Please ensure:

(a) Your request is made in writing to the HR Manager**;**

(b) You enclose the appropriate fee of £10 for provision of the information.

14.2 An initial request that complies with paragraph 14.1 above will be responded to within 40 days of receipt. All information processed using an electronic system and housed in a 'relevant filing system' will be provided.

14.3 If the request is similar or identical to an earlier request the information will not be provided unless a reasonable interval has elapsed since the initial request.

14.4 The Company must be able to say to an employee with certainty that the information they have been provided with from our files is the totality of personal data held relating to them. Accordingly, Managers must ensure that the HR department has a copy of any record of personal data which they hold on an employee in their area of responsibility.

15. Providing information over the telephone

Take care when dealing with telephone enquiries relating to personal information held by us. In particular you 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 you are not sure about the caller's identity and where their identity cannot be checked;

(c) Refer to the Compliance Manager for assistance in difficult situations. You should not be bullied into disclosing personal information.

(d) All requests received for personal data relating to past or present employees must be handled by the HR Advisor. Unlawful disclosure could lead to disciplinary action.

16. Action to be taken if data goes missing

16.1 The Compliance Manager must be informed immediately if any confidential or sensitive data goes missing. An immediate investigation will be launched to discover where the data has gone.

16.2 If it is found that the data has been received by an unauthorised individual it must be determined whether that individual has accessed the data.

16.3 If that individual has and the data was correctly encrypted, compressed and password protected, it suggests that the individual has unlawfully accessed the data. In such situations it might be appropriate to involve the police in the investigation.

16.4 The Compliance Manager will consider whether any individuals need to be informed about the data having gone missing – even if it is subsequently found. This might be necessary if there is a risk of personal data relating to individuals having been sent to the wrong person.

17. Policy Breaches

17.1 Breaches of this policy may result in disciplinary action and, in serious cases, may result in dismissal.

17.2 A number of offences have been created which arise from non-compliance with the provisions and requirements of the Data Protection Act. Examples include unlawful disclosure, unlawful obtaining of data and processing of data without registration.

17.3 These offences are punishable at both the Magistrate's Court and the Crown Court and could lead to a conviction for the Company and/or the individual(s) responsible and a penalty of a potentially substantial fine.

18. Monitoring and review of the policy

18.1 To ensure the policy remains efficient, effective and relevant and consistent with regulatory developments, it will be reviewed by the Compliance Manager in consultation with our legal representatives at least annually.

18.2 Recommendations for any amendments are reported to board.

18.3 Employees are invited to comment on this policy and suggest ways in which it might be improved by contacting the HR Manager.