Henry Boot

DATA PROTECTION POLICY
Version 3 – Updated June 2015

Contents

1. Policy Statement 2
2. The Aims of this Policy 2
3. Handling Personal and Employee Data – Principles of Data Protection 2
4. Implementation of Data Protection Principles 3
5. Employee Data held by the Company 3
6. Use of Employee Data 4
7. Employee Monitoring 5
8. How you can find out what is held by the Company 5
9. How the Company will respond 5
10. Exceptions to your Rights of Access to Personal Data 6
11. Correction of Inaccurate Information 6
12. Employee Procedures for Data Protection 7
13. Effective Date 7
14. Policy Revisions 7

1. Policy Statement

The Company is committed to complying with all aspects of the data protection legislation in its handling of personal information in relation to customers, suppliers and employees. The Company's policy is to ensure that such information is only stored, processed and disclosed when business needs require and, where necessary, to obtain all appropriate consents from individuals who are the subject of such information. The Company is also committed to allowing individuals appropriate access to information held about them and to a regular process of updating and/or destroying out of date information.

2. The Aims of this Policy

In order to operate its business effectively, the Company needs to obtain, use and store information about its customers, suppliers and employees. Data protection legislation controls and limits the collection and use of information which relates to and identifies any person, which is described as "personal data". Both computerised information and paper-based records are covered, provided that the relevant information is filed by reference to that person (i.e. in a file with their name or employee number on it). The Company is committed to best practice in this area and the aims of this policy are threefold:

(a) to educate employees in relation to the Company's approach to handling personal data;

(b) to explain to employees the nature of personal data about them which is held by the Company, the uses to which such data is put and when and how it may be disclosed, and the extent to which employees are entitled to have access to that information, described in this policy as "employee data"; and

(c) to explain to employees what is expected of them in relation to data protection.

3. Handling Personal and Employee Data – Principles of Data Protection

In handling all personal data, including employee data, the Company is committed to complying with the principles of data protection, which are set out below. These require that:

(a) Personal data will be processed fairly and lawfully.

(b) Personal data will be obtained only for specific and lawful purposes as set out in section 1 above, and will not be processed in any manner incompatible with those purposes.

(c) Personal data will be adequate, relevant and not excessive in relation to the purposes for which it is processed.

(d) Personal data will be accurate and where necessary kept up-to-date.

(e) Personal data will not be kept longer than necessary for the purposes for which it is processed.

(f) Personal data will be processed in accordance with the rights of data subjects under the data protection legislation, i.e. providing information about why data is being collected, how information will be used, gaining consent, giving access to data and rectifying inaccurate data.

(g) Personal data will be subject to appropriate technical and organisational security measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.

(h) Personal data will not be transferred to a country or territory outside the European Economic Area, Hungary, Switzerland or the USA (where it is certain that the protocols within the EU-US Safe Harbour Data Exchange Agreement are being followed) unless that country or territory ensures an adequate level of data protection.

4. Implementation of Data Protection Principles

In order to assist in the implementation of these principles, the Company has put in place the following measures:

(a) a Data Protection Officer (see section 14 below) with specific responsibility for the implementation of the data protection principles has been nominated to whom all queries in relation to data protection matters should be directed;

(b) where relevant, employees will undergo training in relation to data protection issues and any employee who feels that he or she requires such training should contact the Data Protection Officer; and

(c) all departments, including the Group HR Department, will be responsible for their own systems of data storage which will ensure that data is held with an appropriate degree of security. That data will only be accessed where strictly necessary and only by those with authority to do so. Appropriate efforts will be made to ensure that all stored data is accurate and updated as necessary and that data which is obsolete or no longer required is destroyed with appropriate regard paid to the confidentiality of that information.

5. Employee Data held by the Company

5.1 The following is a non-exclusive list of examples of formal employee data which the Company is likely to hold on computer or in manual files:

- CVs
- application forms
- test results
- interview notes
- contracts of employment
- medical notes and records
- appraisal records
- accident records
- performance ratings

- training notes
- attendance notes
- payroll records
- disciplinary action or grievance procedures
- redundancy or redeployment records
- pension, pay and compensation
- sales/commission
- financial reference
- equal opportunities-monitoring information
- company car documentation
- medical certificates
- time sheets
- employer references
- next of kin/emergency contacts

5.2 The following is a non-exclusive list of examples of informal employee data which is often of a transitory nature and includes information retained by line managers for day to day management purposes. Whilst covered by this policy it is unlikely to be held on computer or in manual files:

- detailed working rotas
- notes relating to employees' training needs
- notes recording team roles
- notes detailing short-term resource issues
- notes and records of day-to-day matters

6. Use of Employee Data

6.1 The information described above will be available only to the Group IT Manager, the Group's HR personnel and to line managers and directors and will not be disclosed to anyone else, except where strictly necessary (for example in a disciplinary process or in cases of emergency).

6.2 The Company recognises that certain types of data are particularly sensitive. This includes, for example, information in relation to such matters as racial or ethnic origin, trade union membership and physical or mental health or condition. Although inevitably there will be a need for the Company to process sensitive data on occasions, the Company will only do so with the employee's consent, keep as little sensitive information as possible and only where necessary.

6.3 The information will be used for personnel and payroll administration and to answer (inter alia):

- mortgage reference requests and employment or financial references – in both cases after confirmation from the employee concerned; and

- court/legal enquiries and other genuine enquiries.

7. Employee Monitoring

Employees should also be aware that the Company monitors communication and other activities in the following ways:

(a) E-mail facilities and Internet access are provided to employees for business purposes and, therefore, the Company reserves the right to review e-mail messages. Employees should, therefore, not place on the system any message which they regard as personal.

(b) Incoming telephone message may be recorded on internal voicemail systems currently.

(c) The Company records CCTV images using cameras in various external and internal areas. These cameras are installed for the purposes of crime prevention and public and employee safety.

8. How you can find out what is held by the Company

8.1 You have a statutory right to find out what information about you is held on computer and in some paper records. If you want to know whether information is held about you then you will need to write to the Data Protection Officer. You may ask for a copy of all the information held about you to which the data protection legislation applies. The Company, at its discretion, may charge you a fee of up to £10 to cover the administration cost of providing the information you request.

9. How the Company will respond

9.1 The Data Protection Officer will respond in writing to any request for information within 40 days. Subject to the exceptions set out in section 10 below you will be sent a copy of the following information:

(a) a copy of the relevant information constituting the personal data (unless this is not possible, would involve disproportionate effort or you agree to dispense with this requirement);

(b) a description of why the data relating to you was processed;

(c) any other recipients to whom the data may be disclosed (e.g. information about pay being disclosed to the Inland Revenue);

(d) any information available to the Company which relates to the source of the information relating to you; and

(e) provided you expressly ask for it, in relation to data held on computer which forms the sole basis of a decision made by the Company which affects you, the logic involved in making that decision.

9.2 In all cases, the information supplied to you will refer to the data in question at the time the request was received from you. It may take account of any amendment or deletion made between that time and the time when the

information is supplied, provided the amendment or deletion would have been made regardless of your request.

10. Exceptions to your Rights of Access to Personal Data

10.1 In the following circumstances the Company may deny individuals rights of access to information about them:

(a) where compliance with a request for information would result in disclosure of information relating to another individual (unless the third party consents or the Company decides it is reasonable to dispense with that consent);

(b) access to any reference given, or to be given, in confidence by the Company if the reference is to be given for the purposes of the education, training or employment of the employee making the request, or the appointment of any office or the provision of any service by that person;

(c) access to any reference given by a former employer or individual, if given in confidence and the individual who gave the reference does not consent to its disclosure;

(d) data processed for the purposes of management forecasting or planning if it would be likely to prejudice the conduct of the business (eg. data in connection with proposed redundancies or pay reviews);

(e) where the Company is negotiating with the individual making the request (eg. over pay) if access to that information would prejudice the negotiations;

(f) where the Company sets examinations for its employees (eg. as part of their training) the Company need not disclose the results for five months beginning with the date on which the employee asked for the results; and

(g) in any other situation where the Company considers that any of the statutory exceptions apply under the data protection legislation.

11. Correction of Inaccurate Information

The Company recognises that personal data needs to be accurate and, where necessary, kept up to date. If you believe that any personal information held on you by the Company is inaccurate you should write to the Data Protection Officer identifying the inaccuracy and requesting that it is corrected. The Data Protection Officer will respond in writing within 21 days confirming that the inaccuracy has been rectified or otherwise explaining how the matter has been dealt with.

12. Employee Procedures for Data Protection

12.1 All employees have a duty to make sure that they comply with the data protection principles, which are set out above. In particular, employees must ensure that records are accurate, up-to-date, kept and disposed of safely.

12.2 Employees must not disclose personal data to a third party under any circumstances. The only exception will be if an employee of appropriate seniority is satisfied that the disclosure of the personal data is necessary: in the best interests of the employee, or a third person, or the Company and he or she has either informed the individual about whom such data is held of this, or has been unable to do so and disclosure is urgent and necessary, i.e. in exception circumstances, such as a medical emergency. In the event of any doubt as to whether personal data should be disclosed, please contact the Data Protection Officer.

12.3 The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. The Information Security Policy sets out requirements in relation to the security of all Company data, including personal data.

12.4 All employees should ensure that any personal data which they hold is kept securely and personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

12.5 The Company expects all of its employees to comply fully with this Data Protection Policy and the principles of data protection set out in section 3 above.

12.6 Disciplinary action in accordance with the Company Disciplinary & Dismissal Procedure may be taken against any employee who breaches any of the instructions or procedures following from this policy.

13. Effective Date

This policy came into effect on 1st March 2002.

14. Policy Revisions

This policy was revised 10th April 2012 with reference to Social Media and Internet Acceptable Use Policies and Password Policy, and also updated on 1 June 2015.

From 1st April 2015, the role of Data Protection Officer for Henry Boot PLC and its subsidiary companies is held by Amy Oakley, Group Construction Solicitor.