Data Protection Policy

1. POLICY STATEMENT

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.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, customers 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 applicable laws on data protection from time to time in force in England and Wales, including but not limited to the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) 2003, the General Data Protection Regulations (EU) 2016/679 and (once in force) the Data Protection Act 2018, as amended or updated from time to time ("Data Protection Legislation").

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.

2. STATUS OF THE POLICY

This policy has been approved by the Board. It 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.

The Managing Director is responsible for ensuring compliance with Data Protection Legislation and with this policy. That post is held by Wayne Smith, tel: 07903 366420, E-mail: wsmith@heightsconsultancy.co.uk. Any questions or concerns about the operation of this policy should be referred in the first instance to the Managing Director.

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 Managing Director.

3. DEFINITION OF DATA PROTECTION TERMS

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

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.

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), an identifier (such as an identification number or an online identifier), or information about physical, physiological, genetic identity of that person (such as a biometric passport or fingerprint) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who, or organisations which, determine the purposes and means 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 Data Protection Legislation. We are the data controller of all personal data used in our business.

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 security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller.

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.

Sensitive personal data or Special category 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 or special category data can only be processed under strict conditions and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the principles of good practice set out in Data Protection Legislation. These provide that personal data must be:

- Processed fairly, lawfully and transparently;
- Processed for specified, explicit and legitimate purposes and not further processed in a manner which is inconsistent with those purposes;
- Adequate, relevant and limited to what is necessary for the purpose;
- Accurate and kept up to date;
- Not kept longer than necessary;
- Processed in line with data subjects' rights;
- Secure; and
- Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR, LAWFUL AND TRANSPARENT PROCESSING

The Data Protection Legislation is not intended to prevent the processing of personal data but to ensure that it is done fairly and transparently without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case Heights Consultancy Ltd), 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.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the processing is necessary for the performance of a contract or in order to take pre-contract steps, to comply with a legal obligation, to protect the data subject, to perform a task carried out in the public interest or in the exercise of official authority or in the legitimate interest of Heights Consultancy or the party to whom the data is disclosed. Data may also be processed where the data subject has explicitly consented to the processing. When sensitive personal data or special category data is being processed Heights Consultancy will either seek the data subject's explicit consent to the processing or ensure that the more stringent requirements to process such data are met.

6. PROCESSING FOR LIMITED PURPOSES

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 Data Protection Legislation. 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. The data subject must also be informed of their right to object to such additional data processing before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is necessary 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.

8. ACCURATE AND UP-TO-DATE DATA

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.

9. TIMELY PROCESSING

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. For guidance on how long certain data is likely to be kept before being destroyed, contact the Managing Director.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Be informed of what data is processed about them;
- Object to data processing on compelling legitimate grounds;
- Request access to any data held about them by a data controller;
- Prevent the processing of their data for direct-marketing purposes;
- Ask to have inaccurate data amended or removed;
- Prevent processing that is likely to cause damage or distress to themselves or anyone else; and
- Object to automated data processing.

11. DATA SECURITY

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.

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 any a third-party data processor agrees to comply with those procedures and policies or if he puts in place adequate measures himself.

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

· **Confidentiality** means that only people who are authorised to use the data can access it;

· **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed; and

· 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.

Security procedures include:

· **Entry controls**. Any stranger seen in entry-controlled areas should be reported;

· **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.);

· **Methods of disposal**. Paper documents should be shredded. Memory sticks, CD ROMs and the like should be physically destroyed when they are no longer required; and

· **Equipment**. Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock the screen of their PC when it is left unattended.

12. DEALING WITH SUBJECT ACCESS REQUESTS A formal request from a data subject for information that we hold about them must be made in writing. No fee is normally payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to the Managing Director immediately.

13. EMPLOYEE OBLIGATIONS

Employees must ensure that any personal data to which they have access is treated in accordance with these guidelines; in particular, you should not use any such data other than in connection with and to the extent necessary for the purposes of your employment. You should comply with all procedures which we put in place in order to fairly obtain personal data. When inputting data or accessing our database, you must observe any user guidelines, manual or other instructions (issued or amended from time to time) in relation to that database.

Where you collect personal data about individuals from individuals themselves, you must normally tell them what will happen to such data and how it will be used. When obtaining personal data, you must not mislead or deceive data subjects as to the identity of who will be holding their personal data and for what purposes such data will be processed.

If you intend to engage in direct marketing activities, you must give customers an opportunity to state that they do not wish to receive direct marketing material.

If you are in any doubt as to the application of this policy or any obligations relevant to it which affect you, please discuss this with the Managing Director.

14. PROVIDING INFORMATION OVER THE TELEPHONE

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

- Check the caller's identity to make sure that information is only given to a person who is entitled to it;
- 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; and
- Refer to their line manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

15. MONITORING AND REVIEW OF THE POLICY

This policy is reviewed regularly by our Board of Directors. Recommendations for any amendments are reported to the Board.

We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

16. REPORTING OF BREACHES

If you become aware of a breach of this data protection policy or the Data Protection Legislation you must report this to the Managing Director immediately. The Managing Director will determine whether or not it is a personal data breach that is likely to result in a risk to people's rights and freedoms, and will ensure that if so, the breach is reported to the Information Commissioner's Office without undue delay and (where possible) not later than 72 hours of becoming aware of it. The Managing Director will keep a record of any personal data breaches, regardless of whether they need to be reported to the ICO.