Policy Name	**Data Protection Policy**
Purpose	**To ensure that data is dealt with appropriately, ethically, and in line with legislative requirements.**
Applies to	**All Staff**
Date Implemented	**January 2015**

1 Introduction

1.1 In this Policy Arctics Ltd (trading as Igloo) is referred to as the 'Company'. For the avoidance of doubt these rules and procedures should be followed at all times at your individual location of work. In the event that you are placed at a clients' premises you should adhere to their own policies and procedures where they differ to the rules and procedures set out by Igloo.

1.2 The Data Protection Act 1998 (the "Act") enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent and for the purposes for which that data has been provided. The Company is committed to a policy of protecting the rights and privacy of individuals in accordance with the Act.

2 Scope

2.1 This policy applies to all permanent and temporary staff. As a matter of good practice, other agencies and individuals working with the Company, and who have access to personal information, will be expected to comply with the Act. It is expected that those who deal with external agencies will take responsibility for ensuring that such agencies agree to abide by this Act.

3 Aim

3.1 The Company is required to collect and use certain types of information about the people with whom it deals in order to operate. These people include current, past and prospective employees; suppliers; clients/customers; and others with whom it communicates. In addition, the Company may occasionally be required by law to collect and use certain types of information, for example, to comply with the requirements of government departments for business data.

3.2 To comply with the Act, personal information, in any format (paper or electronic) must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

3.3 The Company understands that the lawful and correct treatment of personal information is essential to successful operations, and to maintaining confident relationships with those with whom it deals. The aim of this policy is to ensure that this happens and gives detailed processes to ensure adherence with the Act.

4 Data Protection Definitions

4.1 Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Such data would include name, address, telephone number, hobbies and names of children etc. It would also include expressions of opinion about the individual, and of the intentions of the data controller in respect of that individual.

4.2 Data Controller

Any person (or organisation) that makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

4.3 Data Subject

Any living individual who is the subject of personal data held by an organisation.

4.4 Processing

Any operation related to the organisation, retrieval, disclosure and deletion of data and includes obtaining and recording data, accessing, altering, adding to, merging, and deleting data.

4.5 Third Party

Any individual/organisation other than the data subject, the data controller or its agents

5 Data Protection Principles

5.1 Personal information is processed fairly and lawfully and is not processed unless specific conditions are met.

5.2 Personal information is only obtained for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes.

5.3 Personal information obtained is adequate, relevant and not excessive in relation to the purpose or purposes for which it is required.

5.4 Data is accurate and, where necessary, kept up to date.

5.5 Personal information is not kept for longer than is necessary.

5.6 Personal information is processed in accordance with the rights of the data subjects under the Data Protection Act.

5.7 Appropriate technical and organisational measures are in place to prevent the following:

- Unauthorised or unlawful processing of personal data
- Accidental loss or destruction of personal data
- Damage to personal data

5.8 No personal information is transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6 Data Subject Rights

6.1 An individual has the following rights regarding the processing of any data that is held about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed;
- To prevent processing likely to cause damage or distress;
- To prevent processing for the purposes of direct marketing;
- To be informed about automated decision taking processes that will significantly affect them;
- Not to have significant decisions that will affect them taken solely by automated process;
- To sue for compensation if they suffer damage by any contravention of the Act;
- To take action to rectify, block, erase or destroy inaccurate data; and
- To request the Commissioner to assess whether any provision of the Act has been contravened.

7 Consent

7.1 Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Company understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

7.2 Consent obtained under duress or based on misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication.

7.3 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7.4 If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place

7.5 If an employee is in any doubt about these matters, they should consult their immediate Manager.

8 Security of Data

8.1 All employees are responsible for ensuring that any personal data (on others) which they hold is kept securely and is not disclosed to any unauthorised third party.

8.2 All personal data should be accessible only to those who need to use it. Individuals should form a judgement based upon the sensitivity and value of the information in question, but should always consider keeping personal data:

- in a lockable room with controlled access; or
- in a locked drawer or filing cabinet; or
- if computerised, password protected; or
- kept on disks that are themselves kept securely.

8.3 Care should be taken to ensure that PCs and terminals are not visible except to authorised employees and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where unauthorised personnel can access them.

8.4 This policy also applies to employees who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Employees should take particular care when processing personal data at home or in other locations outside our sites.

9 Rights of Access to Data

9.1 As stated in Para 6.1, individuals have the right to access any personal data that is held about them. This means that Company employees have the right to access any personal information held by the Company in electronic format and manual records that form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Company about that person.

9.2 Any employee who wishes to exercise this right should apply in writing to a director Any such request will normally be complied with within 40 days of receipt of the written request.

9.3 It should be noted that the Company reserves the right to exercise its option [under DPA 98 section 29] to decline subject access requests related to personal information held for the purpose of detection and prevention of crime.

10 Disclosure of Data

10.1 All employees have a responsibility to ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and in certain circumstances, the Police.

10.2 All employees should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose an employee's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose an employee's work details to someone who wished to contact them regarding a non-work related matter.

10.3 The important thing to bear in mind is whether disclosure of the information is relevant to, and necessary for, the conduct of the Company's business.

10.4 This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

- The individual has given their consent;
- The disclosure is in the legitimate interests of the business;
- The Company is legally obliged to disclose the data; or
- Disclosure of the data is required for the performance of a contract.

10.5 The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security;
- To prevent or detect crime, including the apprehension or prosecution of offenders;
- For the assessment or collection of tax duty;
- For the discharge of regulatory functions (includes health, safety and welfare of persons at work);
- To prevent serious harm to a third party; or
- To protect the vital interests of the individual (this refers to life and death situations)

10.6 If an employee receives enquiries for example as to whether a named individual works for the Company, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the employee should decline to comment. Even confirming whether an individual works for the Company may constitute an unauthorised disclosure.

10.7 Unless consent has been obtained, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally, a statement consenting to disclosure to the third party should accompany the request.

10.8 As an alternative to disclosing personal data, the Company may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally i.e. "if the person does work for the Company".

11 Retention of Data

11.1 Data relating to Employees

11.1.1 The Company discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected about employees. However, once an employee has left the Company, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others will.

11.1.2 In general, electronic records containing information about individual employees are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual employees will be kept for 2 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory period of 3 years.

11.1.3 Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. This is to aid management of the recruitment process.

11.2 Data relating to Customers

11.2.1 Databases should not be sold. Databases should be regularly cleaned to ensure that data is not duplicated or spelt incorrectly and only up to date details about customers and prospects are retained. Databases should be maintained to the highest possible standards.

12 Disposal of Records

12.1 All personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

13 Publication of Information

13.1 All employees should be aware that the Company publishes a number of items that include personal data, and will continue to do so. Information published includes:

- Internal Telephone Directory
- Names of members of committees
- Employee information on the Company's website (including photographs)
- Awards
- Newsletters

13.2 It is recognised that there might be occasions when an employee requests that their personal details remain confidential or are restricted to internal access. In such instances, The Company will comply with the request and ensure that appropriate action is taken.

14 Use of CCTV

14.1 Arctics Ltd are registered with the Information Commissioner's Office (ICO) and there are designated personnel across the business who can access data from the CCTV cameras for security, investigation and insurance purposes.

14.2 For reasons of personal security and to protect Igloo's premises and the property of employees and customers, close circuit television cameras are in operation in certain locations. The presence of these cameras may not be obvious. This policy determines that personal data obtained during the monitoring will be processed as follows:

- Any monitoring will be carried out only by a limited number of specified employees
- The recordings will be accessed only by Senior Managers or Directors
- Data is retained for a period of up to 28 days
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete
- Employees involved in monitoring will maintain confidentiality in respect of personal data
- Data obtained may be used within the disciplinary process where required or a report may be provided
- Data may be provided to external regulatory authorities if used as part of an external investigation i.e. Police

14.3 For reasons of personal security and to obtain data in line with Customer/Company contractual obligations, CCTV cameras may be in operation on customer sites in certain locations. This policy also determines that the personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out by their own Data Controller
- A designated individual will be able to access CCTV footage
- Data is retained for a period of up to 28 days
- Data obtained during monitoring will be destroyed as soon as possible after any investigation is complete
- Employees involved in monitoring will maintain confidentiality in respect of personal data
- Data obtained may be used within the disciplinary process where required or a report may be provided
- Data may be provided to external regulatory authorities if used as part of an external investigation i.e. Police

15 Breach of the Policy

15.1 Disciplinary action, up to and including summary dismissal, may be taken if an employee is in breach of this policy.

16 Summary

16.1 The Data Protection Act 1998 gives individuals the right to access the information that an organisation holds on them. In order to comply with this, the Company's needs to have in place effective means of extracting and retrieving information from a variety of sources.

16.2 Departments may hold a great deal of information on employees, usually in a variety of forms and locations. In order to comply with a subject access request, departments will need to be able to locate and collate the information quickly. It is therefore vital that key personnel (typically a Director) know what information is held and by whom.

16.3 Ideally, all information relating to individual employees should be kept in departmental employees' record files (paper or electronic) so that, in the event of a subject access request, The Company can be confident that all the information is easily accessible from a limited number of central sources. However, the Company recognises that this may not always be the case in practice. Departments should ensure that employees' record files are as complete as possible but it is acknowledged that there may be some instances where designated individuals need to retain information on employees that would not be appropriate for more general access.