DATA PROTECTION POLICY

1.0 INTRODUCTION

The Data Protection policy is designed to comply with the Data Protection Act 2018 which came into force on 23rd May 2018. When stating "Data", the organisation is referring to manual and computer based information.

This policy covers two main elements: Employee/Personal Data and Third Party (client) data.

2.0 EMPLOYEE/PERSONAL DATA

2.1 The Data Protection principles are:

- Personal data must be processed fairly and lawfully
- Personal data must be processed for limited purposes and not in any manner incompatible with those purposes
- Personal data must be adequate, relevant and not excessive
- Personal data must be accurate
- Personal data must not be kept for longer than is necessary
- Personal data must be processed in line with data subjects' rights
- Personal data must be secure
- Personal data must not be transferred to any company or countries that don't protect personal data adequately

2.2 Sensitive data is defined within the Act as:

- Racial or ethnic origin
- Political opinions
- Religious and similar beliefs
- Membership of trade unions
- Information on physical or mental health
- An individual's sex life
- Offences committed and any proceedings for any offences that have been committed.

2.3 It is extremely important to the organisation to maintain transparency in relation to data protection. The policy is designed to allow individuals to know who is collecting information on them and how it is to be used and also to ensure information on employees is protected under the Data Protection Act.

3.0 OPERATIONAL PROCESS

This policy is applicable to personal data in computerised, manual or any other format. The policy applies to all aspects of data collected within the organisation.

3.1 Access

All employees have the right to be informed where data is being processed in relation to them. In usual circumstances data on any individual within the organisation will be held on their personnel file and will contain information such as:

- Name
- Date of birth
- Address
- Emergency contact
- National Insurance
- Start date
- Recruitment documentation
- References obtained from a third party
- Bank details
- Sickness records
- Driving Licence and Car Insurance
- Promotional details
- Appraisals
- Remuneration

3.2 It will also retain information on any disciplinary or grievances (see respective policies).

3.3 If an individual wishes to have a copy of the contents of their Personnel file or indeed any other information about them retained by the organisation, then they must apply to Human Resources in writing with their request. The requested information will be provided within 40 days of the request.

3.4 Human Resources will not provide any employee information to a third party unless for the administration of employment (i.e. pensions, professional advisors).

3.5 In addition to "current" employees the data protection policy at the organisation covers individuals who might wish to work for or who have previously worked for the organisation. It therefore includes:

- Applicants (successful and unsuccessful)
- Former applicants (successful and unsuccessful)
- Employees (current and former)
- Casual workers (current and former)
- Contract workers (current and former)

3.6 Bee Lighting is fully committed to setting up methods to protect personal data about employees. In order to ensure this a key person within the organisation is nominated a key person who is responsible for ensuring employment practices and procedures comply with the Act and for ensuring that they continue to do so. The nominated person within Bee Lighting is Colin Fulford.

Managers are made aware of their responsibility in compliance with Data Protection legislation through the implementation of this policy.

3.7 Other parts of the Data Protection policy are:

Employment records

Collecting, storing, disclosing and deleting records

Bee Lighting will only retain information on individual employment records that is relevant to their ongoing employment. Any information that was obtained for recruitment purposes and no longer required will be deleted.

Medical Information

Occupational Health

The organisation will only request medical information once a job offer has been made. This information will be required to enable the organisation to meet its obligations in relation to the safety of its employees and to others to whom it owes a duty of care.

Any information that was obtained for recruitment purposes and no longer required will be deleted.

Retention of Recruitment Records

All general recruitment records will be retained for a maximum period of one year due to the needs of the business.

Any information about criminal convictions collected in the course of the recruitment process will be deleted once it has been verified though a Criminal records Bureau disclosure, unless in exceptional circumstances the information is clearly relevant to the on-going employment relationship.

Human Resources will be responsible for ensuring that any personal data obtained during the recruitment process is securely stored or destroyed.

The organisation will advise unsuccessful candidates that there is an intention to keep their names on file for future vacancies. If any individuals do not wish this to happen they will have an opportunity to express this preference.

References

The organisation may disclose information given in an employment reference to the employee to which it refers, upon request by that person. The organisation's standard reference request incorporates this statement. If there is sufficient justification to refuse to let the employee see the reference obtained on them (i.e. risk of intimidation, violence etc. to the referee), then the request may be refused. The organisation may in certain circumstances contact the referee to discuss in more detail the employee's request to view the reference before a decision is made.

The organisation may refuse to allow an employee to view a reference it has written about them as this situation is an exemption in the Act.

4.0 RESPONSIBILITY

All members of staff have a responsibility to adhere to Data Protection legislation.

If anyone is aware that any member of the organisation is in breach of the Data protection act then they should report the matter immediately to Human Resources.

4.1 Human Resources is responsible for ensuring that the Data protection policy is regularly reviewed in line with updated legislation.

4.2 Employees do have some responsibilities for data protection under this policy. Line managers have responsibility for the type of personal data they collect and how they use them. No workers should disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes. An employee disclosing personal data without the authority of the organisation may commit a criminal offence, unless there is some other legal justification for example under "whistle-blowing" legislation.

5.0 THIRD PARTY/CUSTOMER DATA

5.1 The Data Protection principles in relation to client data are:

- Customer data must be processed fairly and lawfully and stored only on Bee Lighting's data systems.
- Customer data must be processed for business purposes, namely for account management and prospective business leads.
- Customer data must be accurate, adequate and relevant.
- Customer data must be processed in line with data subjects' rights.
- Customer data must be secure.
- Customer data must not be transferred to any company without explicit permission from the customer and within the act's legal bindings.
- Customer data must only be transmitted using a secure method – either a Bee Lighting or Customer approval site. Under new circumstances should data be transmitted using a 3rd party site such as "send this file.com". If in doubt please speak to Colin Fulford.

5.2 It is extremely important to Bee Lighting to maintain transparency in relation to data protection. The policy is designed to allow customers to know what information on them is held, and how it is to be used and also to ensure information on customers is protected under the Data Protection Act.

5.3 **Access**

All customers have the right to request a report of information held on them. All requests must be forwarded to Colin Fulford. Under no circumstances should the report be actioned by the request recipient.

Information under the broader data entities such as:

- Account (Company)
- Contact
- Contracts
- Marketing and Events)
- Activities
- Sales (Orders and Invoices)

5.4 If an individual wishes to have a copy of any of the above the company will respond within 40 days of the request.

5.5 The Company will not provide any customer information to a third party unless for the administration of the customers benefit, and in line with the preferences chosen by the customer.

5.6 The company designated Data Officer as registered with the ICO is Colin Fulford.

6.0 OPERATIONAL PROCESS

This policy is applicable to personal data in computerised, manual or any other format. The policy applies to all aspects of data collected within the organisation.

7.0 RESPONSIBILITY

All members of staff have a responsibility to adhere to Data Protection legislation.

If anyone is aware that any member of the organisation is in breach of the Data protection act then they should report the matter immediately to Colin Fulford.

7.1 All staff have responsibility for the type of customer data they collect and how they use it. No workers should disclose customer data outside the organisation's procedures, use or retain customer data for their own purposes. An employee disclosing customer data without the authority of the organisation may commit a criminal offence, unless there is some other legal justification for example under "whistle-blowing" legislation.