Blossom Ireland

For a Life Like Any Other

Data Protection Policy

Review date: January 2020

1. THE POLICY

1.1 Everyone has rights with regard to how their personal information is handled. During the course of the Company's activities the Company may collect, store and process personal information about staff, service users and service providers, and the Company recognises the need to treat this data in an appropriate and lawful manner. The Company is committed to complying with its obligations in this regard in respect of all personal data it handles.

1.2 The types of information that the Company may be required to handle include details of current, past and prospective employees, suppliers, customers, and others that the Company communicates with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Acts 1988-2003 ('the Acts') and other regulations. The Acts impose restrictions on how the Company may collect and process that data.

1.3 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 up to and including dismissal.

2. PURPOSE AND SCOPE OF THE POLICY

2.1 This policy sets out the Company rules on data protection and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal and sensitive information.

2.2 If an employee considers that the policy has not been followed in respect of personal data about themselves or others they should raise the matter with their manager as soon as possible.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 Data is information which is stored electronically, on a computer, or in certain paper-based filing systems. This would include IT systems and CCTV systems.

3.2 Data subjects for the purpose of this policy include all living individuals about whom the Company holds personal data.

3.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information that is in, or is likely to come into, the possession of the data controller). 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).

3.4 Data controllers are the individual or organisations who control and are responsible for the keeping and use of data.

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

3.6 Processing means performing any operation or set of operations on data, including:

– obtaining, recording or keeping data,
– collecting, organising, storing, altering or adapting the data,
– retrieving, consulting or using the data,
– disclosing the information or data by transmitting, disseminating or otherwise making it available,
– aligning, combining, blocking, erasing or destroying the data.

3.7 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, criminal convictions or the alleged commission of an offence. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

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

(a) Obtained and processed fairly.
(b) Kept only for one or more specified, explicit and lawful purposes.
(c) Used and disclosed only in ways compatible with these purposes.
(d) Kept safe and secure.
(e) Kept accurate complete and up to date.
(f) Adequate, relevant and not excessive.
(g) Retained for no longer than is necessary for the purpose or purposes for which it was collected.
(h) Provided to data subjects on request.

5. OBTAINED & PROCESSED FAIRLY

5.1 The Acts are intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case [Insert Company Name]), the purpose for which the data is to be processed by the Company, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. 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.

6. KEPT FOR ONLY SPECIFIED, EXPLICIT & LAWFUL 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 the Acts. 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. Any employee personal data collected by the Company is used for ordinary Human Resources purposes. Where there is a need to collect employee data for another purpose, the Company will notify the employee of this and where it is appropriate will get employee consent to such processing.

7. USED & DISCLOSED ONLY IN WAYS COMPATIBLE WITH PURPOSE

Personal data should only be collected to the extent that it is required 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. KEPT SAFE & SECURE

8.1 The Company and its employees 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.

8.2 The Acts require the Company to put in place procedures and technologies to maintain the security of all personal data. Personal data may only be transferred to a third-party data processor if the third party has agreed to comply with those procedures and policies or has adequate security measures in place.

8.3 The following must be maintained to ensure the following:

(a) Confidentiality - that only people who are authorised to use the data can access it. The Company will ensure that only authorised persons have access to an employee's personnel file and any other personal or sensitive data held by the Company. Employees are required to maintain the confidentiality of any data to which they have access.

(b) Integrity - that the personal data is accurate and suitable for the purpose for which it is processed.

(c) Availability - that authorised users should be able to access the data if they need it for authorised purposes.

8.4 Security procedures include:

(a) 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.)

(b) Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

(c) 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.

9. ACCURATE & COMPLETE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should 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. Employees should ensure that they notify their manager/Human Resources of any relevant changes to their personal information so that it can be updated and maintained accurately. Examples of relevant changes to data would include a change of address.

10. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. For guidance in relation to particular data retention employees should contact their manager. The Company has various legal obligations to keep certain employee data for a specified period of time. In addition, the Company may need to retain personnel data for a period of time in order to protect its legitimate interests.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

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

(a) Request access to any data held about them by a data controller.
(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. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that the Company holds about them must be made in writing. A fee is payable by the data subject for provision of this information. Any employee who receives a written request in respect of data held by the Company should forward it to their manager immediately. Data subjects should be provided their data in accordance with any such request within 40 days of receiving the request.

13. PROVIDING INFORMATION OVER THE TELEPHONE

13.1 Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the Company over the phone. In particular the employee should:

(a) Check the identity of the caller to ensure sure that information is only given to a person who is entitled to that information.

(b) Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified.
(c) Refer the request to their manager for assistance in difficult situations. No employee should feel forced into disclosing personal information.

14. REVIEW OF POLICY

14.1 The Company will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required taking into account changes in the law and organisational or security changes.

15. TRANSFERRING DATA OUTSIDE THE STATE

As the Company operates internationally OR has third party service providers outside of Ireland, it may be necessary in the course of business that the Company has to transfer an employee's personnel data [within the organisation and/or to other group companies] to countries outside the European Economic Area, which do not have comparable data protection laws to Ireland. The transfer of such data is necessary for the management and administration of the contracts of employment and to facilitate Human Resources administration [within the group]. When this is required, the Company will take steps to ensure that the data has the same level of protection as it does inside of the Republic of Ireland. The Company will only transfer the data to third parties that agree to guarantee the same level of protection.