Version No: 01

Last Updated: April 2018
Review Date: April 2022
Reviewed by: Sandra Roche
Amendments Made: Yes ☐ No ☑

Data Protection Policy

Our commitment

The General Data Protection Regulation and Data Protection Acts 1988-2018 apply to the processing of personal data. Ballymun Job Centre (BJC) is committed to complying with its legal obligations in this regard. The BJC collects and processes personal data relating to its employees in the course of business in a variety of circumstances, e.g., recruitment, training, payment, performance reviews, and to protect the legitimate interests of the organisation. For further information regarding the processing of employee data, please see Ballymun Job Centre's data protection notice.

This policy covers any employee about whom the BJC processes data and includes current and former employees. Processing of data includes: collecting; recording; storing; altering; disclosing; destroying; and blocking. Personal data kept by this organisation shall normally be stored on the employee's personnel file or HR electronic database. Highly sensitive data, such as medical information, will be stored in a separate file, in order to ensure the highest levels of confidentiality. The organisation will ensure that only the HR Manager will have access to an employee's personnel file which is stored in a locked filing cabinet inside the HR Office.

It may be necessary to store certain other personal data outside the HR Office, e.g., salary details will be stored in the accounts office.

In the absence of the HR Manager, the BJC Manager may have access to personal data where necessary.

Collection and storage of data

The BJC processes certain data relevant to the nature of the employment of its employees to comply with relevant legal obligations, to perform the employment contract and, where necessary, to protect its legitimate business interests and the rights and entitlements of employees. We will ensure that personal data will be processed in accordance with the principles of data protection, as described in the GDPR and Data Protection Acts.

Personal data is normally obtained directly from the employee concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties, e.g., references from previous employers. Due to the nature of our work, the BJC may make an application to the Garda Vetting Bureau for Garda clearance of an employee.

Personal data collected by the organisation is used for ordinary HR management purposes, as defined in the first paragraph of this policy. Where there is a need to collect data for another purpose, the BJC shall inform you of this. In cases where it is appropriate to get your consent to such processing, the BJC will do so.

Employees are responsible for ensuring that they inform the HR Manager of any changes in their personal details, e.g. change of address. The Manager will inform the HR Manager of any changes in employees' details, e.g. promotion, pay increases. We endeavour to ensure personal data held by the organisation is up to date and accurate.

Retention of data

The BJC is under a legal obligation to keep certain data for a specified period of time. In addition, the organisation will need to keep personal data for a period of time in order to protect its legitimate interests. For further information regarding relevant retention periods, employees should refer to the BJC data retention policy.

Security and disclosure of data

The BJC will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Security measures will be reviewed from time to time, having regard to the technology available, the cost and the risk of unauthorised access. Employees must implement all organisational security policies and procedures, e.g. use of computer passwords, locking filing cabinets, not leaving information on desks etc.

HR files are stored in the HR office and employees who have access to these files must ensure that they treat them confidentially. Employees working in the payroll/accounts department must treat all personal data they receive confidentially and must not disclose it, except in the course of their employment.

All employees will have access to a certain amount of personal data relating to colleagues, clients and other third parties. Employees must play their part in ensuring its confidentiality.

They must adhere to the following data protection principles:

- Process data fairly, lawfully and transparently

• Keep data only for specified, explicit and legitimate purpose(s)

• Process data only in ways which are compatible with the purpose(s) for which it was given

• Ensure data is accurate and up-to-date

• Ensure data is adequate, relevant and limited to what is necessary for the purpose for which it was given

• Keep data safely and securely

• Retain personal data for no longer than is necessary for the purpose for which it is processed and in line with the company's data retention policy

Employees must not disclose personal data, except where necessary in the course of their employment, or in accordance with law. They must not remove or destroy personal data except for lawful reasons and with the permission of the organisation.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal. If employees are in any doubt regarding their obligations, they should contact the Data Protection Officer/HR Manager.

Medical data

The BJC does not carry out pre-employment medicals as part of the recruitment process. Occasionally, it may be necessary to refer employees to a doctor for a medical opinion and all employees are required by their contract of employment to attend in this case. The organisation may receive certain medical information, which will be stored in a secure manner with the utmost regard for the confidentiality of the document.

Employees are entitled to request access to their medical reports. Should an employee wish to do so, please contact the HR Manager, who will consult with the doctor who examined you and request the data. Employees are required to submit sick certificates in accordance with the sick leave policy. These will be stored by the BJC having the utmost regard for their confidentiality.

E-mail monitoring

The BJC provides e-mail facilities and access to the internet. In order to protect against the dangers associated with e-mail and internet use, screening software is in place to monitor e-mail and web usage. Mailboxes are only opened:

- upon specific authorisation by a manager in cases where the screening software or a complaint indicates that a particular mailbox may contain material that is dangerous or offensive;

- where there is a legitimate work reason or in the legitimate interest of the BJC.

Please refer to the e-mail and internet usage policies for further details.

Data Protection Officer

Sandra Forbes is the Data Protection Officer for the Ballymun Job Centre. She is responsible for assisting the organisation in monitoring and maintaining compliance with data protection legislation. All employees must co-operate with the data protection officer when carrying out her duties.

The data protection officer is also available to answer queries or deal with employees' concerns about data protection.

Access requests

Employees are entitled to request data held about them on computer or in relevant filing sets. The BJC will, in most circumstances provide this data within one month. In some cases, due to the complexity of the request or the number of requests being handled by the organisation, the organisation may require a further two months to provide this data. There is no charge for requesting this data.

An employee should make a request in writing to the data protection officer, stating the exact data required. Employees are only entitled to access data about themselves and will not be provided with data relating to other employees or third parties. It may be possible to block out data relating to a third party or conceal his or her identity, and if this is possible the organisation may do so.

Data that is classified as the opinion of another person will be provided unless it was given on the understanding that it will be treated confidentially. Employees who express opinions about other employees in the course of their employment should bear in mind that their opinion may be disclosed in an access request, e.g., performance appraisals.

In some circumstances where relevant exemptions apply, certain personal data may not be provided to an employee. An employee will be informed where personal data is not being disclosed on the basis of such an exemption.

An employee who is dissatisfied with the outcome of an access request has the option of using the organisation's grievance procedure. He/she may also refer a complaint to the Data Protection Commissioner.

Right to object

Employees have the right to object to data processing that is causing them distress and/or to correct personal data which is inaccurate. Where such objection is justified, the BJC will cease processing the data unless it has a legitimate interest that prevents this. The organisation will make every effort to alleviate the distress caused to the individual.

An objection should be made in writing to the data protection officer, outlining the data in question and the harm being caused to the employee.

Transmission of data outside the State

It may be necessary in the course of business to transfer employee's personal data within the organisation and to other organisations in countries outside of Ireland. This relates mainly to employees working on EU Projects and the transfer of such data is necessary for the management and administration of EU Projects and funding. When this is necessary, the organisation will take steps to ensure that the data has the same level of protection as it does inside the State. The organisation will only transmit to companies that agree to guarantee this level of protection. For more information, please contact the data protection officer.

Review

This policy will be reviewed from time to time to take into account changes in the law and the experience of the policy in practice.

Next Review Date: May 2024