

Data Protection Policy

Policy Statement

Basingstoke ITEC Limited (the company) intends to fully comply with all requirements of the Data Protection Act 1998 as far as it affects the company's activities, including updated requirements under the General Data Protection Regulation.

Scope

This Data Protection Policy:

- Covers the processing of all personal information whose use is controlled by the company
- Covers all personal information handled, stored, processed or shared by the company whether stored in physical or I.T based record systems
- Applies to all employees, volunteers, learners, customers and other individuals it may come into contact with during the normal course of business

Introduction

In order to be able to conduct business and meet the requirements of the Education and Skills Funding Agency contract, rules and regulations, Basingstoke ITEC Limited will lawfully collect and process certain information (including where required sensitive personal data) about its employees, volunteers, learners, customers (including suppliers) and other individuals it may come into contact with during the normal course of business. In collecting and using this data, the company is committed to protecting an individual's rights to privacy with regard to the processing of this personal data.

This policy sets out the rules that all Basingstoke ITEC Limited employees, volunteers, learners and customers (including suppliers) who process or use any personal information on behalf of the company are subject to, in order to ensure it is compliant with its obligations under the Act.

The Act governs that there is a valid lawful basis in order to process personal data; this must be fair and transparent. Under GDPR, the data protection principles set out the main responsibilities for organisations; Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals
2. collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in public interests, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GPRD in order to safeguard the rights and freedoms of individuals
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The company, its employees, volunteers, learners and customers (including suppliers) who process or use any personal data on behalf of the company must comply with these principles and ensure that they are followed at all times.

Responsibilities

The legal responsibility for compliance with the Act is with Basingstoke ITEC Limited who is the data controller under the Act and is registered as such with the Information Commissioner's Office (Registration Number: Z6453774). Responsibility for compliance is delegated to senior management members who are responsible for encouraging data processing best practice within the company. However, compliance with this policy and the Act is the responsibility of everyone within the company who processes personal information.

Failure to follow this policy may result in disciplinary proceedings.

Individual Consent

In most cases, Basingstoke ITEC Limited can only process personal data with the consent of the individual whom the data concerns. However, it is a condition of learner enrolment and staff employment that they agree to the company processing certain personal information as a part of the company's statutory obligations – see also the ESFA Privacy Notice:

<https://www.gov.uk/government/publications/esfa-privacy-notice>

The company may process some information that is categorised as 'sensitive personal data'; this includes information about an individual's racial or ethnic origin, gender, physical or mental health and criminal convictions, charges or proceedings. This information may be required to comply with certain government or funding body regulations, to ensure safety or to meet the company's policies and procedures.

Information Disclosure

Basingstoke ITEC Limited requires all employees, volunteers, learners and customers (including suppliers) to be vigilant and exercise caution when asked to provide personal data held on another individual. In particular, they must not disclose any personal information either orally or in writing to any unauthorised individual, which includes family members and friends, without the express prior consent of the relevant individual.

Data Security

All employees, volunteers, learners and customers (including suppliers) must ensure that any personal data they hold is kept securely and that they take appropriate security precautions by seeking to ensure:

- source documents are kept in a lockable cabinet or draw or room
- computerised data is password protected
- data kept on discs or data storage devices are stored securely and encrypted
- ensure individual passwords are kept confidential and are not disclosed to other personnel enabling log-in under another individual's personal username and password
- logged on PCs are not left unattended where data is visible on screen to unauthorised personnel
- screensavers are used at all times
- paper-based records must never be left where unauthorised personnel can read or gain access to them

When manual records are no longer required they should be shredded and the hard drives of redundant PCs should be wiped clean.

Off-site use of personal data presents a greater risk of loss, theft or damage and the company and personal liability that may accrue from off-site use of personal data is similarly increased. For this reason employees and others should:

- only take data off-site when absolutely necessary and for the shortest time possible
- take particular care when laptops or personal machines are used to process personal data at home or in locations outside of the company – that they are to be kept secure at all times

Personal Data Breach

A personal data breach means a breach of security leading to the destruction, loss, altering, unauthorised disclosure of or access to personal data.

If Basingstoke ITEC Limited discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner **within 72 hours of discovery**.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, Basingstoke ITEC Limited will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures taken.

A breach may include but is not limited; a risk to the rights and freedoms of individuals which could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is not likely to result in a risk to the rights and freedoms of individuals, Basingstoke ITEC does not need to notify the Information Commissioner, or the individuals affected.

Basingstoke ITEC Limited must keep a record of all data breaches, whether reportable or not.

All third-party processors must notify Basingstoke ITEC Limited of all incidents without undue delay. If there is a risk to rights and freedoms of an individual; Basingstoke ITEC Limited will inform that individual unless:

- Breach is unlikely to result in high risk for the rights and freedoms of individuals;
- Appropriate technical and organisational protections were in place; or
- Would trigger disproportionate efforts

Rights of Individuals

The GDPR provides the following rights for individuals:

1. to be informed about information collected and use of their personal data, including the purpose for processing their personal data, retention periods and who it can be shared with
2. request access to information held on them, the purpose for which the information is being used and those to whom it is, has or can be shared with
3. to request rectification on inaccurate personal data, or completion if incomplete
4. to have personal data erased, also known as the 'right to be forgotten', this is not absolute and only applies in certain circumstances
5. to request restricted or suppression of personal data, this is not absolute and only applies in certain circumstances
6. data portability allows individuals to obtain and reuse their personal data for their own purposes across different services, this allows them to move, copy or transfer

personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability

a. unless:

- i. the company can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- ii. the processing is for the establishment, exercise or defence of legal claims

7. to object to the processing of personal data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics

8. be informed about the reasons behind any automatic decision making and profiling

Access to Personal Data

Subject to exemptions, the Act gives any individual who has personal data kept about them by Basingstoke ITEC Limited the right to request in writing a copy of the information held relating to the individual in electronic format and also in some manual filing systems. Any person who wants to exercise this right should in the first instance make a written request to the company General Manager.

After receipt of a written request, any information needed as proof of identity of the person making the request, Basingstoke ITEC Limited will ensure that the individual receives access within 40 calendar days, unless there is a valid reason for delay or an exemption is applicable.

The Act does not prevent an individual making a subject access request via a third party, including by a solicitor acting on behalf of a client. In these cases and prior to the disclosure of any personal information, Basingstoke ITEC Limited would need to be satisfied that the third party making the request is entitled to act on behalf of the individual and would require evidence of this entitlement.

Whilst the Act does not limit the number of subject access requests an individual can make to any organisation, Basingstoke ITEC Limited is not obliged to comply with an identical or similar request to one already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

Direct Marketing

Under the Act an individual has the right to prevent his/her personal data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not begin) using their personal data for direct marketing. Any individual can exercise this right, and if Basingstoke ITEC Limited receives a notice then it must comply within a reasonable period.

Any marketing campaign should be permission-based with a clear explanation of what an individual's details will be used for and a simple way should be included for an individual to opt out of marketing messages.

Accuracy of Data

Staff are responsible for:

- ensuring that any information they provide to the company relating to their employment is accurate and up to date
- informing the company of any information changes, eg. change of address
- checking the information that the company may send out from time to time giving details of information kept and processed about staff

Learners must also ensure that all data provided to Basingstoke ITEC Limited is accurate and up-to-date by notifying their assessor.

Basingstoke ITEC Limited cannot be held responsible for any errors unless the member of staff or learner has informed the company about them.

Retention and Disposal of Data

Basingstoke ITEC Limited is not permitted to keep personal information of either learners or staff for longer than is required for its purpose. However, some data will be kept longer or in perpetuity to comply with statutory or funding body requirements.

Personal and confidential information will be disposed of by means that protect the rights of those individuals i.e. shredding, disposal of confidential waste, secure electronic deletion.

Complaints

Basingstoke ITEC Limited is dedicated to being compliant with the Act. Individuals, any member of staff or learners wishing to report concerns relating to the Act should, in the first instance, contact the General Manager or the Funding and Contracts Manager.