Data Protection Policy

Document Version Control			
Document Version	**Date**	**Policy Author(s)**	**Review Date**
Version 1.0	01/07/2017	Joe Turner	01/07/2018

Introduction

Bluestone College processes personal data in relation to its own staff, learners and individual client contacts. It is vitally important that we abide by the principles of the Data Protection Act 1998 set out below.

Bluestone College holds data on individuals for the following general purposes:

- Staff Administration
- Advertising, marketing and public relations
- Accounts and records
- Administration and processing of work-seekers personal data for the purposes of work-finding services

The Data Protection Act 1998 requires Bluestone College as data controller to process data in accordance with the principles of data protection. These require that data shall be: -

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subjects rights
- Kept securely
- Not transferred to countries outside the European Economic Area without adequate protection.

Personal data means data, which relates to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of, Bluestone College.

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data, which does not amount to processing. It applies to any processing that is carried out on computer including any type of computer however described, main frame, desktop, laptop, palm top etc.

Data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date and those people listed in the appendix shall be responsible for doing this.

Data may only be processed with the consent of the person whose data is held. Therefore if they have not consented to their personal details being passed to a third party this may constitute a breach of the Data Protection Act 1998. By instructing Bluestone College to look for work and providing us with personal data contained in a CV, work-seekers will be giving their consent to processing their details for work-finding purposes. If you intend to use their data for any other purpose you must obtain their specific consent.

However caution should be exercised before forwarding personal details of any of the individuals on which data is held to any third party such as past, current or prospective employers; suppliers; customers and clients; persons making an enquiry or complaint and any other third party.

Data in respect of the following is "sensitive personal data" and any information held on any of these matters MUST not be passed on to any third party without the express written consent of the individual:

- Any offence committed or alleged to be committed by them
- Proceedings in relation to any offence and any sentence passed
- Physical or mental health or condition
- Racial or ethnic origins
- Sexual life
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Whether someone is a member of a trade union

Retention of Data

Bluestone College will keep some forms of information for longer than others. The Data Retention Policy provides details of the recommended and statutory periods. Data on students, including any information on health, race or disciplinary matters, will be destroyed after ten years but a skeletal record will be retained to include a full transcript of academic achievements.

Records of assessment will be retained for a period of 3 years in line with the requirements of Ofqual.

Data Security

All staff are responsible for ensuring that any personal data, which they hold, is stored securely, for example:

- Kept in a locked filing cabinet; or
- In a secure staff area; or
- In a locked drawer;
- If it is computerised, be password protected; or
- Kept only on disk, which is itself kept securely;
- Is not generally taken home.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

From a security point of view, only those staff listed in the appendix should be permitted to add, amend or delete data from the database. However all staff are responsible for notifying those listed where information is known to be old, inaccurate or out of date. In addition all

employees should ensure that adequate security measures are in place. For example adopting and following a clear desk policy:

- Computer screens should not be left open by individuals who have access to personal data
- Passwords should not be disclosed
- Email should be used with care
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason.
- Personnel files should always be locked away when not in use and when in use should not be left unattended
- Any breaches of security should be treated as a disciplinary issue.
- Care should be taken when sending personal data in internal or external mail
- Destroying or disposing of personal data counts as processing. Therefore care should be taken in the disposal of any personal data to ensure that it is appropriate. For example, it would have been more appropriate to shred sensitive data than merely to dispose of it in the dustbin.

It should be remembered that the incorrect processing of personal data e.g. sending an individual's details to the wrong person; allowing unauthorised persons access to personal data; or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/or negligence leading to a claim against Bluestone College for damages from an employee, learner or client contact. A failure to observe the contents of this policy will be treated as a disciplinary offence.

Data subjects, i.e. those on whom personal data is held, are entitled to obtain access to their data on request and after payment of a fee. All requests to access data by data subjects i.e. staff, members, customers or clients, suppliers, students etc should be referred to Joe Turner whose details are also listed on the appendix to this policy.

Any requests for access to a reference given by a third party must be referred to Joe Turner *a*nd should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with the Data Protection Act 1998, and not disclosed without their consent. Therefore when taking up references an individual should always be asked to give their consent to the disclosure of the reference to a third party and/or the individual who is the subject of the reference if they make a subject access request. However if they do not consent then consideration should be given as to whether the details of the individual giving the reference can be deleted so that they cannot be identified from the content of the letter. If so the reference may be disclosed in an anonymous form.

Finally it should be remembered that all individuals have the following rights under the Human Rights Act 1998 and in dealing with personal data these should be respected at all times:

- Right to respect for private and family life
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly and association
- Freedom from discrimination