GDPR policy

Data Controller

Business Education Events Ltd (BEE) is the Data Controller and determines the purposes for which and the manner in which any personal data are, or are to be processed. Lisa Quinn, Director acts as Data Protection Officer and takes responsibility for data on a daily basis.

Data Protection policy statement

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act 2018 - the UK's implementation of the General Data Protection Regulation (GDPR). Everyone at BEE responsible for using personal data has to follow strict data protection principles. They must make sure the information is: used fairly, lawfully and transparently. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

BEE collects a small amount of personal data each year including: examination marks of students on our mentoring projects, proof of identity documents for Mentor DBS checks, references, and names and contact details of business volunteers.

2. BEE adheres to the following in the processing of personal data. Information is:

GDPR policy

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

3. Responsibilities

3.1 BEE must:
Manage and process personal data properly
Protect the individuals' right to privacy
Provide an individual with access to all personal data held on them.

3.2 BEE has a legal responsibility to comply with the Act.

3.3 BEE is registered with the Information Commissioner's Office of the processing of personal data. Our registration number is: 0484 000 2259

3.4 Every member of staff that holds personal information has to comply with the Act when managing that information.

3.5 BEE is committed to maintaining the principles at all times. This means that BEE will:

GDPR policy

• inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice

• check the quality and accuracy of the information held

• apply the record's management policies and procedures to ensure that information is not held longer than is necessary

• ensure that when information is authorised for disposal it is done appropriately

• ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system

• only share personal information with others when it is necessary and legally appropriate to do so

• set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act

• train all staff so that they are aware of their responsibilities

This policy will be updated as necessary.

GDPR policy

Procedure for Access to Personal Information / Business Education Events (BEE)

Rights of access to information

There are two distinct rights of access to information held by BEE about students and business volunteers.

1. Under the Data Protection Act 1998 a person has a right to request access to their own personal information. In certain circumstances requests may be made by a parent on behalf of their child (see below).

2. The right of parents to have access to curricular and educational records relating to their child as defined within the Education (Pupil Information) (England) Regulations 2005.

These procedures relate to the above-mentioned rights.

Dealing with a request

1. Requests for personal information must be made in writing and addressed to the BEE's Data Controller (Lisa Quinn) If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any personal information

Evidence of identity can be established by requesting production of: passport; driving licence; utility bills with the current address; Birth / Marriage certificate; P45/P60; Credit Card or Mortgage statement. This list is not exhaustive.

GDPR policy

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand. As a general rule, a child of 12 or older is expected to be mature enough to understand the request they are making. If the child cannot understand the nature of the request, someone with parental responsibility can ask for the information on the child's behalf. BEE would discuss the request with the school, or person with parental responsibility and take their views into account when making a decision.

4. The response time for subject access requests, once officially received, is 40 days.

5. Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another individual involved should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

Complaints

Complaints about the above procedures should be made to Karen O'Connor, Director at BEE who will decide whether it is appropriate for the complaint to be dealt with in accordance with BEE's complaint procedure.

Complaints which are not appropriate to be dealt with through BEE's complaint procedure can be dealt with by the Information Commissioner.

Data Retention Policy

A vital part of BEE's Data Protection Policy and practice is that personal data is retained for the appropriate period of time. We will not retain personal data for longer than is necessary to fulfil the purposes for which we collected that personal information, unless the law permits or requires that we retain it for longer. We will always take all reasonable precautions to make sure that data remains secure and is handled in accordance with our data protection policy. Data that is provided to us is stored on our secure

GDPR policy

servers. Details relating to any transactions, or personal details relating to DBS checks or student information will be kept on a secure hard drive, or in the unlikely event of it needing to be transferred, we will encrypt the data to ensure its safety. The transmission of information via the internet is not completely secure and where necessary we will create passwords for excel spreadsheets that contain sensitive personal details and/or encrypt data transfer.

	Type of Data Held	Location of Data	Source of Data	Reason for Data Being Held	Retention Period	Reason for Retention Period	Delete/ Anonymise
Students / Learners (Mentee specific *in italics)*	• Full name • Dates of Birth • Race, religion, sexual orientation (anonymised data) • *Medical information (i.e. information relating to disabilities or medical information that mentors may need to know about mentees)* • CVs • Qualifications	Hard drive	Schools, or students themselves in mentee interviews / mock interview events requiring CVs	To ensure records are up to date and accurate	*Information kept for as long as the programme endures: e.g. CVs sent 5 weeks before a mock interview event and will be deleted afterwards; mentor programmes last for circa 10 months	*Medical records are classed as sensitive personal data and will be deleted once the mentoring relationship has ceased*	Anonymise / delete
Volunteers (Mentor specific *in italics)*	• Full name • Dates of volunteering • Dates of Birth • *Full address* • *Previous Address* • Telephone numbers	Hard drive	Volunteers or CSR leads in individual companies	To ensure records are up to date and accurate	Information updated every 2 years with opt out included	• *Previous address* • *information may be needed for a short period after it has*	Delete

GDPR policy

	• Email address • *Copy of driving licence, bank information, birth certificate and/or other identifying documents* • *References*					*been changed to confirm previous address history, and for DBS checks* • *Identifying documents deleted upon the DBS certificate being issued to mentor* • *References: 6 years after having left employment*	
Employees	• Full name • Dates of Birth • Race, religion, sexual orientation (anonymised data) • Next of kin and emergency	Hard drive	Employee	Contractual Obligations	6 years after having left employment	Claims can be brought up to 6 years after the end of employment, so this information may be needed in the event of a claim being brought.	Delete

GDPR policy

Processor policy

Karen O'Connor, Director, is the person in charge of deleting data or disposing of hardware data that may have been kept on.

Research from the ICO (during 2016) revealed that 40% of UK data security incidents were attributed to paper. These include:

- 19% Data posted/ faxed to wrong recipient
- 14% Loss/theft of paper work
- 4% Data left in insecure location
- 3% Insecure disposal of paperwork

Since then, 2017 has seen a further 20% increase in loss or theft of paperwork, thus heightening the importance of ensuring paper-based security protocols within all businesses. BEE has taken the decision to commit to cross cut shredding in the erasure of data as a result. Karen O'Connor is in charge of the internal data breach log for when/if mistakes occur. Karen O'Connor will put into action our processes if we ever have to report a breach to the ICO.