GENERAL DATA PROTECTION & PRIVACY POLICY

Introduction

In May 2018 the General Data Protection Regulation (GDPR) replaced the Data Protection Act of 1998 and brought about the biggest change to data protection laws in over 20 years. In general it introduced stricter rules on how firms and organisations handle and use of personal data. In particular, the new directive takes aim at how sensitive customer information is processed, stored and exchanged among businesses.

The act concentrates on personal data and the main differences is on how we get, keep and protect personal data. It applies to all organisations within the EU holding information about individuals worldwide and worldwide organisations must protect personal data for all EU citizens, personal data kept on identifiable individuals i.e. all personal data relating to living individuals that is held on either computer database or in a structured paper filing system. GDPR gives more power to people over how their personal data is used and make it easier for them to access it.

1. Purpose of Data Protection and Privacy Policy

Beacon East is a company supporting young people in schools and colleges with careers guidance. Consequently, Beacon East staff/associates will use student data as part of their daily work. Beacon East is fully committed to ensuring compliance with existing GDPR regulations. The company recognises the importance of personal data to its business of Careers & IAG in schools and colleges and the importance of respecting the privacy rights of individuals. Beacon East is also fully aware of the ICO (The information Commissioner's Office) and works very hard to adhere to their principles of the importance data protection. The ICO is the UK's independent public body set up to promote access to official information and protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken. For more information on ICO go to www.ico.org.uk

This company policy sets out the principles which it applies to the processing of personal data so that the company and associates not only safeguard one of it's most valuable assets but also process personal data in accordance with the law. Beacon East works in accordance, and adheres to, the data protection polices of all schools and colleges with which the company works. Where information has been provided to the school by a third party, for example by the local authority, the police, a health care professional or another school, but is held on the school's file it is normal to seek the consent of the third party before disclosing information. Where Beacon East acts on behalf of the school in this capacity it will make sure it adheres

to the policies and wishes of not only the school but the third party e.g. Norfolk County Council and use of Help You Choose data.

It is the responsibility of all Beacon East staff/associates and any person holding or processing personal data on behalf of the company to comply with this policy. Staff, associates and relevant persons should familiarise themselves both with this policy and guidance and apply the provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to the dismissal of staff. Serious breaches could also result in personal criminal liability. This policy continues to apply to individuals even after their relationship with the company ends.

In addition, a failure to comply with this policy could expose the company to enforcement action or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public. For these reasons, it is important that all associates, staff and relevant persons familiarise themselves with this policy and guidance and attend all training sessions in respect of care and handling of personal data.

The Data Protection Act 1998 Principles:

The Act sets out eight principles to be complied with when personal data is processed. These principles are as follow:

(1) Personal data shall be processed fairly and lawfully.

(2) Personal data shall be obtained only for one or more specified and lawful purposes and must not be further processed in any manner incompatible with those purposes.

(3) Personal data shall be adequate, relevant and not excessive.

(4) Personal data shall be accurate and where necessary kept up-to-date.

(5) Personal data shall not be kept for longer than is necessary.

(6) Personal data shall be processed in accordance with the rights of data subjects. These rights are: The right of subject access, The right to prevent processing likely to cause damage or distress, The right to prevent processing for purposes of direct marketing, The right to object to automated decision-taking.

(7) Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

(8) Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This policy applies to all personal data used or processed by the company however it is collected, recorded and used and whether it is on paper records or computer records.

In this policy, “processing” means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) Organisation, adaptation or alteration of the information or data

(b) Retrieval, consultation or use of the information or data

(c) Disclosure of the information or data by transmission, dissemination or otherwise making available

(d) or alignment, combination, blocking, erasure or destruction of the information or data.

(e) and “processed” shall be construed accordingly.

Some definitions:

Data Subject: The individual i.e. students, teachers, mentees you are working with. They have rights to access information kept on them. Data protection will be even stricter when it comes to handling personal data of children. The idea is that they may be less aware of risks and consequences of dishing out sensitive information about themselves and should therefore be afforded to heightened protection compared to adults.

Data Controller: Those collecting the information, i.e. advisers and associates have a legal responsibility to keep personal data safe and secure.

Data Processor: Organisation responsible for keeping records. For advisers it will be the school, college or training provider you are working with. For staff/associates it will be the main organisation, Beacon-East.

2. Types of data we Process

We process personal data about young people we are working with in schools but also staff, associates, business contacts, school and college colleagues and contractors.

The personal data we process takes different forms. It may be factual information, expressions of opinion, images or other recorded information which identifies or relates to a living individual. Examples include:

- Names, addresses, telephone numbers, e-mail addresses and other contact details
- family details, if applicable
- Academic, disciplinary and other education related records, information about special educational needs, if applicable
- Education and employment data
- Images, audio and video recordings
- Financial information
- Courses, meetings or events attended

When working with schools we may, from time to time, need to process special category personal data (e.g. concerning health, ethnicity, religion or biometric data) and criminal records information about some individuals (particularly pupils and staff). We do so in accordance with applicable law (including with respect to safeguarding or employment) or by explicit consent.

3. Obtaining data

Beacon East staff/associates will use data obtained by the school, college or third party such as local authority. Beacon East rarely asks for an additional data. If Beacon East did obtain other data it would fully adhere to principles of the Data Protection Act 1998. The company recognises this will need permission of the client, their parents/guardians and other stakeholders. It also recognises there is a requirement of any data collection form used in order to collect personal data will contain a “fair obtaining” or “privacy” statement. The statement will need to be clearly visible on this form and placed appropriately so the data subject (individual to whom the information relates) is fully aware of the intended uses of their personal data.

In line with GDPR legislation we will monitor and record consent as part of new record keeping processes. This consent will also be features in all future correspondence and marketing materials as well as featured on our website.

4. Handling and Sharing Personal data

Beacon East staff/associates collect most of the personal data we process directly from the individual concerned (or in the case of young people, from their school or college). In some cases, we collect data from third parties e.g. local authorities, professionals/authorities working with the individual or from publicly available resources.

Personal data held by us is processed by appropriate members of staff for the purposes for which the data was provided. We take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems.

Purposes for which we process personal data

Beacon East staff/associates administration including the recruitment of staff, engagement of contractors (including compliance with DBS procedures); administration of payroll, review and appraisal of staff performance; conduct of any grievance, capability or disciplinary procedures; and the maintenance of appropriate human resources records for current and former staff; and providing references;

The promotion of Beacon East through its own websites, publications and communications (including through our social media channels).

The processing set out above is carried out to fulfil our legal obligations (including those under our parent contract and staff employment contracts). We also expect these purposes to form our legitimate interests.

5. **Preventing abuse and discrimination**

Beacon East staff/associates will at times use and/or process sensitive personal client data (as defined in the Data Protection Act). The company will have regard to its various diversity and equality policies to ensure that if instances of data discrimination occur, appropriate action is taken.

Sensitive Personal Data consists of the following information:

Racial or ethnic origin of the client. Client's political opinions/beliefs. Client's religious beliefs or other beliefs of a similar nature. Client's Trade Union membership. Client's physical or mental health condition. Client's sexual orientation. Client's commission or alleged commission of any offence. Any proceedings for any offence committed or alleged to have been committed. **N.B sensitive personal data is subject to much stricter conditions of usage/processing.**

6. **Recording and Using the Data**

Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the client. The company will endeavour to inform all individuals of why their personal data is being collected. In line with the first Data Protection principle, any requested information will be

collected fairly and lawfully and processed in line with the purpose for which it has been given i.e. careers guidance.

The company may need to hold and process the information in order to carry out any statutory obligations, where this process takes place all personal data will be processed fairly and lawfully. It will not be taken away from the place or work i.e. school or college.

The company will endeavour to ensure that information kept is accurate and relevant. Where it is found that information is inaccurate, remedial steps will be taken. Personal client data will be kept no longer than is necessary and will be kept securely at the school or college. The company can also process personal data if it has the consent of the school, college or third party e.g. Local Authority.

7. Ensuring Compliance to current GDPR legislation

Beacon East's Quality Assurance Team annually undergoes a full review of current practice to ensure we are compliant with legislation by conducting an annual Information Audit Map to review current data processing and record keeping.

8. Confidentiality and Security

Beacon East staff/associates must not access, copy, alter, interfere with or disclose personal data held by the school or college without official authorisation.

Access to and use of personal data held by the school or college is only permitted to Beacon East associates and staff for the purpose of carrying out their official duties. Use for any other purpose is prohibited and any breach may result in disciplinary or legal proceedings.

Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles. Confidential information can be the most valuable asset of a school or college and associates/employees will automatically have duties to their clients to ensure that confidential information is not knowingly or recklessly misused. Individuals that process personal data must comply with school or college security measures to safeguard personal data as outlined in their Data Protection Polices. Beacon East associates/employees when using third party data e.g. Local Authority must comply with school or college security measures to safeguard personal data as outlined in their Data Protection Polices.

How long will we keep personal data?

Beacon East will retain personal data only for a legitimate and lawful reason and only for so long as necessary or required by law. We have adopted Records Retention Guidelines which set out the time period for which different categories of data are kept.

Any Beacon East associates, staff or relevant person who becomes aware of a weakness in data protection procedures or who becomes aware of any breach of the policy must report the concern to their line manager (Mark Bruhin) and the relevant person at the institution they are working in. This must be done at the earliest opportunity in order to prevent any further breaches.

9. Disclosing data

Personal data must not be disclosed to anyone internally or externally, unless the person disclosing the information is fully satisfied that the requestor is authorised and legally entitled to the information. Personal data may be disclosed to authorised persons if required under one of the exemptions within the Data Protection 1998. These exemptions are contained within The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (S.I. No 419).

10. Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Mark Bruhin – contact details below.

Depending on the lawful basis above, you may also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

11. Withdrawal of consent and the right to lodge a complaint

Where Beacon East are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting Mark Bruhin, details below.

12. Data Protection Officer

The company contact for data protection is Mark Bruhin who can be contacted at:

E Mail: mbruhin@beacon-east.co.uk Tel: 01603 673340 / 07766 056330

Mark Bruhin is the first point of contact on any aspects of this policy document. Mark Bruhin is also responsible for dealing with data protection enquiries.

The Data Protection Officer has a number of roles:

- Ensure advisers and associates of their obligations in complying with GDPR
- Monitoring compliance by:
- Managing internal data protection
- Awareness raising
- Conduct internal audits
- Handling Data Breach incidents and complaints

13. Breach Notification

Beacon East has procedures in place to detect, report and investigate a personal data breach. In the first instance if you expect a data breach has occurred is to notify Mark Bruhin (see contact details above).

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.