Data Protection Policy

1. Introduction

This Policy sets out the basis on which ABP will collect and use Personal Data either where the ABP collects it from individuals itself, or where it is provided to ABP by third parties. It also sets out rules on how the ABP handles, uses, transfers and stores Personal Data.

Policy applies to all staff, volunteers or those processing data on behalf of ABP. This policy applies regardless of where the data is held i.e. if the personal data is held on personally-owned equipment or outside ABP property. This policy also applies to any expression of opinion about an individual, personal data held visually in photographs or video clips (including CCTV), and sound recordings.

The document provides the policy framework through which effective management of Data Protection matters can be achieved. The purpose of this policy is to ensure that ABP and its staff comply with local laws as well as the stipulations in the European Union's General Data Protection Regulation when processing personal data.

ABP is the data controller. ABP holds personal data about students, parents, staff and other individuals in order to carry out its business and provide its services. For example, this information could include name, address, email address and date of birth. No matter how it is collected, recorded and used, this personal information must be dealt with properly to ensure compliance with data protection legislation.

2. Definitions

2.1 Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.2 Data Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

2.3 Data Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2.4 Personal Data: any information relating to an identified or identifiable natural person.

2.5 Data Subject: an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.6 Processing Data: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other making available, alignment or combination, restriction, erasure or destruction.

2.7 Sensitive Personal Data: data revealing ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data, data containing health or a person's sex life or sexual orientation.

3. Principles of Data Protection

3.1 Any member of staff processing personal data must comply with the six principles described below. The principles require that personal data shall be:

3.1.1 Processed lawfully, fairly and in a transparent manner in relation to individuals;

3.1.2 Collected for specific, explicit and legitimate purposes 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;

3.1.3 Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;

3.1.4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay;

3.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes 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 the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the individuals;

3.1.6 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.

3.2 Additionally, ABP also requires that the data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

4. Roles and Responsibilities

4.1 ABP's responsibilities are to:

4.1.1 Establish policies and procedures and ensure that they are up to date and comply with the law;

4.1.2 Ensure that staff know about and understand this policy;

4.1.3 Provide staff with data protection training.

4.2 The Compliance Officer's responsibilities are to:

4.2.1 Handle subject access requests;

4.2.2 Investigate data protections breaches;

4.2.3 Draw up guidance on good data protection practice;

4.2.4 Advise staff with data protection queries.

4.3 Staff responsibilities are to:

4.3.1 Comply with this policy and any other supporting policies and procedures;

4.3.2 Only access the personal data of others that they need to use;

4.3.3 Make sure their own personal data provided to ABP is accurate and up to date;

4.3.4 Inform ABP if any of their personal data changes;

4.3.5 Inform ABP if they become aware that any of the information that ABP holds about them is not accurate;

4.3.6 Ensure all personal data is kept securely;

4.3.7 Ensure no personal data is disclosed either verbally or in writing to any unauthorised third party. Ensure personal data is kept in accordance with ABP's retention schedule;

4.3.8 ABP will retain learners' data for up to 2 years;

4.3.9 Promptly direct any queries regarding data protection, including subject access requests, to the Compliance Officer;

4.3.10 Inform the Compliance Officer of any data protection breaches as soon as possible and support the Compliance Officer in resolving breaches.

4.4 Learners and other users' responsibilities are:

4.4.1 Make sure that any personal data that they provide is accurate and up to date;

4.4.2 Inform ABP if any of their personal data changes;

4.4.3 Inform ABP if they become aware that any of the information that ABP holds about them is not accurate;

4.5 Individual Rights:

4.5.1 ABP is dedicated to ensuring that the rights of individuals about whom information is held can be fully exercised. These rights are:

4.5.2 The right to be informed;

4.5.3 The right to access;

4.5.4 The right to rectification;

4.5.5 The right to erasure (the right to be forgotten);

4.5.6 The right to restrict processing;

4.5.7 The right to data portability;

4.5.8 The right to object;

4.5.9 The rights related to automated decision-making including profiling.