ABLAZE
DATA PROTECTION POLICY

Introduction

Ablaze recognises the importance of respecting the personal privacy of all our employees, contractors, trustees, partners and service users and the need to build in appropriate safeguards during the collection, storage, processing, and utilisation of personal data.

Personal data is any significant item of information relating to a former, current, or potential Employee, Trustee, Partner or Customer. The Company will principally collect and maintain such data in order to meet its legitimate interests as an employer and business, and to comply with statutory requirements.

Ablaze is registered as a data controller under the GDPR 2018. The Company's Data protection officer is Julia Thomas, Trustee.

Principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

I. processed lawfully, fairly and in a transparent manner in relation to individuals;

II. collected for specified, 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;

III. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

IV. 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 purposes for which they are processed, are erased or rectified without delay;

V. 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 the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and 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, Purposes for holding personal data.

The purposes for holding personal data are for:

i) Recruitment, training, and career development.

ii) Calculation and transfer of payroll data. (This includes details of bank/building society accounts for salary transfers and the payment of authorised expenses).

iii) Determination and calculation of certain benefits including pensions.

iv) For contacting next of kin or emergency contact and arranging medical attention for an employee whilst at work.

v) Compliance with statutory requests from HM Revenue & Customs, The Department of Social Security, The Benefits Agency, and other relevant public authorities/agencies.

vi) Disciplinary purposes arising from an employee's conduct or ability to perform their job.

vii) Provision of references to potential future employers, financial institutions or educational establishments. Information will only be provided following receipt of written consent from the employee.

viii) Confirming the eligibility of all new and potential employees to work in the UK. A copy of relevant documentation will be held on the individual's personnel file.

ix) Confirmation of any consent obtained in order to request a medical report on an individual employee.

x) Utilizing the volunteers to complete the charity work agreed when they signed up for the scheme.

xi) Brokering relationships and organising programme delivery for students in educational settings

xii) Managing programme delivery for students; this includes registers of attendance, group organisation and timetables, evaluation data, universal permission and consent forms.

Personal Identifiers (Personal Data):

The following sensitive information ('sensitive personal data') is subject to statutory restriction and will only be held on file for specific, legitimate purposes. Sensitive personal data will be kept separate from other personnel records relating to the individual employee:

i) Information relating to racial or ethnic origin, sex or sexual orientation, age, religious or philosophical beliefs. This will be collected, with the express consent of each individual concerned, for strictly statistical purposes in connection with equal opportunities monitoring.

ii) Sickness absence records, information relating to any medical condition or illness of an employee which may affect their ability to perform their job or data obtained to comply with the Equality Act 2010 will be kept in strict confidence by the Data protection officer. Such information will be collected and retained only with the express consent of the individual employee and removed when no longer valid or relevant. This information will only be shared with authorised persons.

Data Security

Employees and Contractors may be in possession of personal information about customers, colleagues, members of the public and suppliers. All such information whether held on manual or computerised systems must be kept strictly confidential and treated with care.

Employees and Contractors are responsible for ensuring that:

i) Any manual personal data which they hold is kept securely in locked filing cabinets or cupboards.

ii) Personal data is not disclosed either verbally or in writing or otherwise to any unauthorised third party or without the consent of the individual concerned.

iii) Wherever possible, personal data, and in particular sensitive data should not be e-mailed or faxed unless proper security measures are in place, such as password protection.

iv) No personal data should be disclosed by telephone. Requests should be obtained in writing and proof of identity verified.

v) Any new filing system or computer database which may be set up by an employee and which contains personal data is covered by the Company's notification entry.

vi) A back-up is made of any personal data and is held securely by the Company.

vii) Passwords, access codes and other authorisation used to access personal data are safeguarded. At least one other person should be aware of any passwords you set up.

viii) Computer screens cannot be seen by unauthorised persons and you log off at all times when you are away from your workstation.

ix) Any personal data held on files or on laptops which are taken away from the office are kept securely, and under no circumstances accessible to any unauthorised persons

If you are unsure about how to deal with any request for information, you should ask your manager for guidance. The penalties under the GDPR for wrongful disclosure are quite severe and even accidental disclosure may have implications for you personally.

Access to personal data

Volunteers, employees and people involved with Ablaze will be asked on an annual basis to confirm the personal details we hold on you.

In order to ensure our records are kept up to date, you must inform the Data protection officer immediately of any changes to your personal details or circumstances.

Everyone whose personal details are held by the charity has the right to access those details, subject to some specific exceptions.

If you wish to view the personal information held about you, you should contact the Data protection officer to arrange a convenient date and time. Your request will be dealt with within the statutory time limits and generally within 10 working days of your request.

Your personal file will be reviewed by the Data protection officer to ensure that any documents with restricted access as detailed below are removed and placed in a sealed envelope with a list of contents on the front. During the review, any information that is no longer relevant will be destroyed. A note will be made on the file that it has been reviewed.

The Company has the right to withhold:

i) Information in the case of unreasonably regular requests from you

ii) Specific information where we cannot comply with your request except by disclosing information about another individual.

iii) Any data which is excluded through legislation on grounds of national security, or is relevant to any current investigation concerning any possible criminal/civil legal action.

You have the right to make any reasonable request for the amendment of your own record provided that:

i) You can demonstrate an identifiable error, necessary update or relevant omission.

ii) It is unlawful to maintain such a record.

Any request to correct or amend your records should be made in writing to the Data protection officer within ten working days of accessing your records.

No record may be altered or removed without the express permission of the Data protection officer.

Access to personal information relating to any employee, contractor or partner from a third party will only be given if said person has explicitly given explicit consent.

Right to Object

You are entitled at any time, by notice in writing, to require us to cease within a reasonable time from processing any personal data because it is causing, or is likely to cause, substantial damage or distress to you or another individual. The reasons for this request must be clearly stated and be fully justified.

Customer Information

The principles of the GDPR extend to information held by the Company on its customers and any other third party who is an individual. The Act does not apply to data held in respect of companies.

Ablaze Resources will inform its customers of the uses to which the information it holds about them may be put and to whom any information may be disclosed such as regulatory authorities.

Any customer has the right to request access to data held in a 'relevant filing system' i.e., the information is referenced to the individual or is structured in such a way that the information relating to a particular individual is readily accessible. This can be held in an electronic or manual form.

Customers wishing to have access to personal data (i.e., data relating to an identifiable person) should request this in writing to the Data protection officer. Any employee who is notified of such a request must immediately forward this to the Data protection officer.

If a customer supplies the Company with personal data, including sensitive personal data, relating to a third party, the customer should be made fully aware of its responsibilities to comply with the relevant data protection laws including obtaining consent for the disclosure and use of such data, as appropriate.

Breach of Policy

In the unlikely event of a data security breach, the following actions are immediately carried out under the direction of a responsible officer:

- *Containment*: immediately ensure that no further breaches can occur e.g., by securing hard-copy materials, having IT systems expertly checked for malware, implementing changes and changing passwords.
- *Assessment of the risks*: immediately establish what data has been compromised and the specific risks associated with this breach. Evaluate the potential adverse consequences for individuals based on these specifics; how serious or substantial are these risks and how likely they are to happen.
- *Damage limitation*: inform those individuals potentially affected (their parents where data affected pertains to under-18s) and ensure they are aware of their need to take appropriate steps such as monitoring communications and changing passwords.
- *Wider notification of breach*: based on the assessed risks, a responsible officer then determines whether it will aid damage limitation if other parties such as the police, other relevant agencies or the media are informed, and implements decisions accordingly.
- *Evaluation and response*: investigate the causes of the breach and the effectiveness of the response to it. Update policies and procedures accordingly.

When a breach of data protection occurs, consideration will be given to reviewing practices. In addition, Ablaze will consider whether the breach should be reported to the information commissioner's office.