**Believe Alternative Provision – GDPR and Data Protection Policy**

**Data Protection Officer – Eve Richards**

**1. Introduction:**

1.1 Data protection laws protect individuals from the misuse of information about them. The rapid spread of the internet and ownership of electronic devices made it easier for data to be collected and modernised legal provisions are needed to limit data spread only to those who need to know.

In order to comply with the law there is a requirement for Believe Alternative Provision to have a lawful basis in order to process personal data.

To do this, Believe Alternative Provision must comply with the General Data Protection Regulations 2018 (GDPR) and the Data Protection Act 2018.

1.2 The General Data Protection Regulation (GDPR)

The GDPR gives people rights to access information held about them. In addition, there are obligations for better data management and a regime of fines. The UK government is committed to implementing the GDPR irrespective of Brexit. Employers must ensure they are data protection compliant.

The Data Protection Act 2018 (DPA)

The DPA and GDPR contain rights concerning the processing of personal data which is held in either a computerised format as part of a database or manual records forming part of a relevant filing system. In essence, the law means that those who decide how and why personal data is processed (data controllers) must comply with certain principles. Those whose data is held or processed (data subjects) have rights, for example in relation to accessing that data. In an employment context, employers will generally be data controllers and employees, workers, ex-employees and applicants will be data subjects. Most HR and employment files and records are covered by the DPA.

1.3 Processing data

Processing data includes obtaining, holding, retrieving, consulting and using data by carrying out any operation on it. There are six key principles which specify for example that data must be limited, processed fairly and collected for specified and legitimate purposes.

The principles are broadly similar to the principles in the Data Protection Act 1998 (the 1998 Act).

| 1998 Act | GDPR |
|---|---|

| | |
|---|---|
| Principle 1 - fair and lawful | Principle (a) - lawfulness, fairness and transparency lawful |
| Principle 2 - purposes | Principle (b) - purpose limitation |
| Principle 3 - adequacy | Principle (c) - data minimisation |
| Principle 4 - accuracy | Principle (d) - accuracy |
| Principle 5 - retention | Principle (e) - storage limitation |
| Principle 6 - rights | No principle - separate provisions in Chapter lll |
| Principle 7 – security | Principle (f) - integrity and confidentiality |
| Principle 8 – international | No principle - separate provisions in transfers Chapter V |
| (no equivalent) | Accountability principle |

1.4 lmportant Note: The GDPR extends the scope of legislation to include written and printed material, not just electronic data.

Believe Alternative Provision and all of its staff, or others who process or use any personal information, must ensure that they follow these principles at all times. ln order to ensure that this happens, Believe Alternative Provision has developed this Data Protection, GDPR and Retention of Records Policy.

**2. What is defined as personal data?**

2.1 Personal data relates to someone who can be identified, directly or indirectly, by an 'identifier' such as their name, or an identification number, or by location. lt also includes people who can be identified by various factors in online data. HR records, including sickness absence, performance appraisals, recruitment notes etc. Are personal data.

Sensitive personal data includes information about an individual's race, ethnicity, politics, religion or beliefs, trade union status, health, sex life, sexual orientation or crimes. Genetic or biometric data (for example, fingerprint images for security or payment systems) are included. lt is legitimate to process ‘sensitive personal data' where necessary to carry out an obligation under an employment contract or collective agreement.

Criminal records are sensitive data. Checks are permissible for roles that involve working with children or vulnerable adults but cannot be carried out routinely.

Health information should only be held with explicit consent. Processing medical records may be permissible for preventative steps, assessing working capacity or confirming diagnoses.

When handling personal data, organisations must have safeguards on confidentiality. Any request for data must state why the organisation is collecting the information, what will happen to it and who will see it.

**3. Status of the policy:**

3.1 This policy is incorporated in Believe Alternative Provision's formal contract of employment. Infringement of the requirements of this policy may result in disciplinary action being taken. If any of Believe Alternative Provision's staff, volunteers, members or service providers consider that this Policy has not been followed, in respect of personal data about themselves, they should raise the matter initially with the designated Data Controller. If the matter is not resolved it should be raised as a formal grievance.

**4. Responsibilities of staff:**

4.1 All staff are responsible for:

- checking that any information that they provide to Believe Alternative Provision in connection with their employment is accurate and up to date
- informing Believe Alternative Provision of any changes to information which they have provided, e.g. changes of address
- informing Believe alternative provision of any errors or changes in staff information.

4.2 If and when, as part of their responsibilities, staff collect information (i.e. personal information, opinions about ability, or details of personal circumstances) about other people or members, they must comply with any guidelines which may be published. In particular, they must seek the permission of the Data Controller for their proposed information collection and uses.

4.3 The Director has overall responsibility and is responsible for monitoring the steps taken to ensure that the Act and this Policy are complied with. Particular care must be taken when work is being undertaken externally or when an existing body of material is being brought within Believe Alternative Provision for the first time.

**5. Data security and storage:**

5.1 All staff are responsible for ensuring that:

- Any personal data, which they hold, or for which they are responsible, is kept securely,

  for example:

  - Kept in a locked filing cabinet;
  - In a locked drawer;
  - If it is computerised, be password protected
  - If computerised, then the computer itself is kept in suitably secure conditions.
  - Data should not be stored on the hard drives of desktop personal computers but on the networked storage facilities provided.
  - Where it is necessary to store information on laptop computers (or offsite) then the machine must at all times be maintained physically secure. Where the data is particularly sensitive, consideration must be given to the adoption of additional security measures which would protect the information in the event of the loss or

theft of the computer. Care must be taken to ensure that data is frequently transferred to network storage and that discrepancies are not allowed to arise.

- Where information is to be gathered through, or used on, a website then appropriate measures must be in place to control access and prevent unauthorised disclosure.

5.2 Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. (With the exception of vulnerable adults and children or others at risk)

5.3 Advice on the collection, retention and secure storage of information may be obtained from the Data Controller

5.4 Staff should note that unauthorised disclosure is a breach of the Data Protection Act and may result in disciplinary action. In some cases it may be considered as gross misconduct. It may also result in a personal liability for the individual staff member.

**6. Rights to access information:**

6.1 Employees and other users / members of Believe Alternative Provision have the right to access any personal data that is being kept about them either on computer or in other types of files. Should any person wish to exercise this right they should contact the Data Controller.

6.2 In order to gain access, a request should be made in writing to the Data Controller.

6.3 Believe Alternative Provision aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days. (See SAR procedure)

**7. Subject consent:**

7.1 In many cases, Believe Alternative Provision can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, express consent must be obtained. Agreement to Believe Alternative Provision processing some specified classes of personal data is a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Ad 1974.

7.2 Therefore, all prospective staff will be asked to consent to their data being processed when an offer of employment is made.

**8. Processing sensitive information:**

8.1 Sometimes it is necessary to process sensitive information about a person such as race, gender or family details. This is done to ensure that Believe Alternative Provision can operate policies on matters such as sick pay or equal opportunities. Believe Alternative Provision may also ask for information about particular health needs or disabilities. Believe Alternative Provision will only use such information in the protection of the health and safety of the individual, but will need consent to process: for example in the event of a medical emergency.

Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, employees and others affected will be asked to give express consent for Believe Alternative Provision to do this.

**9. The Data Controller:**

9.1 The designated Data Controller will deal with the implementation of the agreed policy and day to day matters.

9.2 Believe Alternative Provision designated Data Controller is the Director Eve Richards

**10. Retention and destruction of data:**

10.1 Believe Alternative Provision will keep some forms of information longer than others. Believe Alternative Provision will need to keep central personnel records for 6 years after employment ceases. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. All other documents and paperwork will be retained only as long as necessary.

10.2 Believe Alternative Provision will only keep student/pupil data during their enrolment in the provision. After provision ends Believe Alternative Provision will return all documentation to their main education setting or the commissioner of the service within 3 months of the end of provision. All duplicate documentation will be destroyed within 3 months of the provision ending.

10.3 Believe Alternative Provision will carry out the following methods for destruction of data:

- For Paper: Data will be shredded then incinerated through a third-party body who are fully compliant with the GDPR and Data protection laws and will provide a certificate of destruction on completion.
- For Electronic Data including back-ups: Data will be deleted using Secure deletion software to overwrite data one or more times. Electronic hardware will be physically destroyed through a third-party body who are fully compliant with the GDPR and Data protection laws and will provide a certificate of destruction on completion.

10.4 Believe Alternative provision allows for data to be anonymised for reporting or analysis rather than destroyed, where it is feasible and relevant.

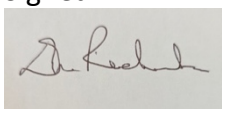
**11. Conclusion:**

11.1 Compliance with the Data Protection Act 2018 and the General Data Protection Regulations is the responsibility of all staff, volunteers, trustees and members of Believe Alternative Provision. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to Believe Alternative Provision's facilities being withdrawn, or even a criminal prosecution.

11.2 Any questions or concerns about the interpretation or operation of this Policy should be taken up with the Data Controller.

**Related Documents:**
See Data Protection Information Legislation

Signed



Date 01/09/2025

Eve Richards
Director and Data Protection Officer - Believe Alternative Provision

Date of Review: September 2026