

Beacon Alternative Provision

Data Protection and Privacy Policy



1. Introduction

Beacon Alternative Provision is committed to protecting the privacy and security of personal data. This policy outlines our compliance with the General Data Protection Regulation (GDPR), data handling and storage procedures, and the privacy rights of students and staff.

2. Purpose

The purpose of this policy is to:

- Ensure compliance with GDPR and other relevant data protection legislation.
- Outline the procedures for handling and storing personal data.
- Inform students and staff of their privacy rights.

3. Scope

This policy applies to all personal data processed by Beacon Alternative Provision, including data related to students, staff, and any other individuals.

4. GDPR Compliance

4.1 Lawful Basis for Processing

- **Consent:** Personal data is processed based on the consent of the data subject, which must be freely given, specific, informed, and unambiguous.
- **Contractual Necessity:** Data may be processed if it is necessary for the performance of a contract with the data subject.
- **Legal Obligation:** Processing may be required to comply with legal obligations.
- **Legitimate Interests:** Data may be processed if it is necessary for the legitimate interests of Beacon Alternative Provision, provided these interests are not overridden by the rights and freedoms of the data subject.

4.2 Data Protection Principles

Beacon Alternative Provision adheres to the following principles when processing personal data:

- **Lawfulness, Fairness, and Transparency:** Data is processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation:** Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data Minimisation:** Data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy:** Data is accurate and, where necessary, kept up to date.
- **Storage Limitation:** Data is kept in a form which permits identification of data subjects for no longer than is necessary.
- **Integrity and Confidentiality:** Data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

4.3 Data Protection Officer

Beacon Alternative Provision has appointed a Data Protection Officer (DPO) who is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

5. Data Handling and Storage Procedures

5.1 Data Collection

- **Transparency:** Data subjects are informed about the purposes of data collection, the legal basis for processing, and their rights through clear and accessible privacy notices.
- **Consent:** Where consent is required, it is obtained through a clear, affirmative action by the data subject.

5.2 Data Storage

- **Secure Storage:** Personal data is stored securely using appropriate technical and organisational measures to protect against unauthorised access, alteration, disclosure, or destruction.
- **Access Controls:** Access to personal data is restricted to authorised personnel only.

5.3 Data Retention

- **Retention Periods:** Personal data is retained for the period necessary to fulfil the purposes for which it was collected, or as required by law.
- **Disposal:** Personal data that is no longer needed is securely deleted or destroyed.

5.4 Data Sharing

- **Third Parties:** Personal data is only shared with third parties who have a legitimate need to know, and where appropriate safeguards are in place.
- **Data Processing Agreements:** Third parties that process data on behalf of Beacon Alternative Provision are required to sign data processing agreements to ensure GDPR compliance.

6. Student and Staff Privacy Rights

6.1 Right to Be Informed

Data subjects have the right to be informed about the collection and use of their personal data. Beacon Alternative Provision provides this information through privacy notices.

6.2 Right of Access

Data subjects have the right to access their personal data and obtain information about how it is being processed. Requests for access should be made to the DPO.

6.3 Right to Rectification

Data subjects have the right to have inaccurate personal data corrected or completed if it is incomplete.

6.4 Right to Erasure

Data subjects have the right to request the deletion of their personal data in certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected.

6.5 Right to Restrict Processing

Data subjects have the right to request the restriction or suppression of their personal data under certain conditions.

6.6 Right to Data Portability

Data subjects have the right to obtain and reuse their personal data for their own purposes across different services.

6.7 Right to Object

Data subjects have the right to object to the processing of their personal data in certain circumstances, including direct marketing.

6.8 Rights Related to Automated Decision Making and Profiling

Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

7. Breach Reporting

- **Reporting:** All data breaches must be reported immediately to the DPO.

- **Investigation:** The DPO will investigate the breach and take appropriate action to mitigate the effects and prevent recurrence.
- **Notification:** Where required, the DPO will notify the Information Commissioner's Office (ICO) and affected data subjects.

8. Review of the Policy

This policy will be reviewed annually to ensure it remains up to date and compliant with relevant legislation. Any necessary amendments will be made in consultation with staff and other stakeholders.

By adhering to this policy, Beacon Alternative Provision ensures the protection of personal data, upholds the privacy rights of individuals, and maintains compliance with GDPR and other relevant data protection regulations.