Beacon Alternative School CIC (and Alternative Provision)

Data Protection Policy

Date: January 2026
Written by: O'Connell/Field
Review Due by: January 2027

Note: Beacon Alternative Provision operates under **Beacon Alternative School CIC**, which is not currently a registered school but is working toward future registration. This policy applies to all staff working with young people across all Beacon settings.

Contents
1. Introduction
2. Aims and Principles
3. Scope of the Policy
4. Legal Framework
5. Data Protection Principles
6. Lawful Basis for Processing
7. Types of Data Collected
8. Data Storage and Security
9. Data Sharing
10. Data Retention
11. Individual Rights
12. Data Breaches
13. Roles and Responsibilities
14. Training and Awareness
15. Monitoring and Review
16. Related Policies

1. Introduction

Beacon Alternative School CIC is committed to protecting the privacy and personal data of young people, families, staff, and partners. We recognise that many of the young people we work with are vulnerable and that the careful, respectful handling of personal information is essential to safeguarding, trust, and effective support.

This policy outlines how personal data is collected, used, stored, shared, and protected in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Aims and Principles

Beacon's approach to data protection aims to:
- Protect the rights and privacy of individuals
- Ensure personal data is handled lawfully, fairly, and transparently
- Safeguard sensitive and special category data
- Support effective multi-agency working while maintaining confidentiality
- Ensure staff understand their responsibilities when handling data

Data protection at Beacon is underpinned by practices that are:
- Proportionate and purposeful
- Trauma-informed and respectful
- Secure and confidential
- Appropriate to a small, relational Alternative Provision setting

3. Scope of the Policy

This policy applies to:
- All staff, including temporary, agency, and sessional staff
- Volunteers and contractors
- Young people attending Beacon
- Parents and carers
- Partner organisations where data is shared

It applies to all forms of personal data, including electronic records, paper files, emails, photographs, and verbal information.

4. **Legal Framework**

This policy is based on the requirements of:
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- Relevant education, safeguarding, and child protection legislation

5. **Data Protection Principles**

Beacon processes personal data in accordance with the seven data protection principles. Personal data must be:
- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Kept only for as long as necessary
- Processed securely
- Handled in a way that demonstrates accountability

6. **Lawful Basis for Processing**

Beacon processes personal data under one or more of the following lawful bases:
- Public task – to provide education, support, and safeguarding
- Legal obligation – including safeguarding, attendance, and reporting duties
- Vital interests – to protect a young person's welfare
- Consent – where required, such as for photographs or social media use

Special category data is processed where necessary for safeguarding, education, and support purposes, in line with statutory requirements.

7. **Types of Data Collected**

Beacon may collect and process the following types of data:
- Young people's data, including names, dates of birth, contact details, attendance, behaviour, progress, SEND information, medical and safeguarding records
- Parent and carer data, including names, contact details, and relationship to the young person
- Staff data, including employment records, DBS checks, training records, and payroll information
- Only data that is necessary and relevant is collected.

8. **Data Storage and Security**

Beacon takes appropriate technical and organisational measures to protect personal data, including:
- Secure, password-protected digital systems
- Restricted access on a need-to-know basis
- Locked storage for paper records
- Secure handling of devices and documents

Staff are expected to follow confidentiality and data security procedures at all times.

9. **Data Sharing**

Personal data may be shared with relevant external agencies where lawful and necessary, including:
- Local Authorities
- Referring schools
- Safeguarding partners
- Health and social care professionals
- Commissioning bodies

Data sharing is limited to what is necessary and is carried out in line with safeguarding and data protection requirements.

10. **Data Retention**

Personal data is retained only for as long as necessary, in accordance with:
- Statutory guidance
- Safeguarding requirements

- Local Authority retention schedules

Data is securely disposed of when no longer required.

11. Individual Rights

Under UK GDPR, individuals have the right to:
- Access their personal data
- Request correction of inaccurate data
- Request erasure, where applicable
- Restrict or object to processing in certain circumstances

Requests should be made in writing and will be responded to within statutory timescales.

12. Data Breaches

Any actual or suspected data breach must be reported immediately to the Headteacher / Data Protection Lead.

Beacon will:
- Investigate the breach promptly
- Take steps to reduce risk and harm
- Report to the Information Commissioner's Office (ICO) where required

13. Roles and Responsibilities

The Headteacher / Proprietor has overall responsibility for data protection compliance.
The Data Protection Lead oversees day-to-day data protection matters, including requests and breach management.

All staff are responsible for handling personal data securely and in line with this policy.

14. Training and Awareness

All staff receive guidance and training on:
- Confidentiality and data protection expectations
- Secure handling of information
- Recognising and reporting data breaches

Training is refreshed as required.

15. Monitoring and Review

This policy is reviewed annually, or sooner if required due to changes in legislation or operational practice.

16. Related Policies

- Safeguarding and Child Protection Policy
- Assessment and Feedback Policy
- Behaviour Policy
- SEND Policy
- Staff Code of Conduct