Beacon Alternative School CIC (and Alternative Provision)

Cyber Security 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 Beacon AP sites, including home-based teaching locations and approved off-site venues. It applies to all students, staff, volunteers, and visitors while under Beacon's duty of care.

1. Introduction

Beacon Alternative Provision recognises the importance of protecting digital systems and personal data from cyber threats. As a small, flexible organisation working with vulnerable young people, Beacon holds sensitive information that must be managed securely and responsibly.

This policy sets out how Beacon protects digital systems and data, reduces cyber risk, and responds appropriately to cyber incidents.

2. Purpose

This policy aims to:
- Protect personal, sensitive, and safeguarding data
- Reduce the risk of cyber attacks and data breaches
- Ensure safe and responsible use of technology
- Support compliance with data protection legislation
- Provide clear guidance for staff and students

3. Scope

This policy applies to:
- All staff, including sessional and temporary staff
- Volunteers and contractors
- Students using Beacon technology

It applies to:
- Beacon-owned or managed devices
- Personal devices used for Beacon work
- Cloud-based systems, email, and digital platforms
- Remote and home-based working

4. Legal and Regulatory Framework

This policy is informed by:
- UK GDPR
- Data Protection Act 2018
- Keeping Children Safe in Education (KCSIE)
- National Cyber Security Centre (NCSC) guidance

5. Information and Data Security

Beacon processes personal and sensitive data, including:
- Student and family contact details
- SEND, safeguarding, and medical information

- Attendance, behaviour, and progress records
- Staff records

Data is:
- Stored securely
- Accessed only on a need-to-know basis
- Protected by passwords and appropriate security measures
- Handled in line with the Data Protection Policy

6. Roles and Responsibilities

Head of Provision
Overall responsibility for cyber security and compliance.

Information Security Lead
Day-to-day oversight of cyber security and incident response.

Staff
Follow this policy, protect login details, and report concerns immediately.

Students
Use technology safely and report anything that feels unsafe or suspicious.

7. Access and Password Security

Beacon requires:
- Strong, unique passwords
- Passwords not to be shared
- Devices to be locked when unattended
- Two-factor authentication where available

Staff must not store passwords insecurely or allow others to access Beacon systems.

8. Devices and Software

Beacon ensures that:
- Devices are password-protected
- Operating systems and software are kept up to date
- Antivirus and security software are used where appropriate

Lost or stolen devices must be reported immediately.

9. Email, Internet, and Phishing

Staff and students must:
- Be alert to phishing emails or suspicious messages
- Avoid clicking unknown links or downloading attachments
- Report suspicious activity immediately

Cyber awareness is supported through guidance and training.

10. Remote and Home Working

When working remotely, staff must:
- Use secure Wi-Fi connections
- Avoid using public or unsecured networks where possible
- Ensure devices are not accessible to others
- Log out of systems when not in use

11. Data Storage, Backup, and Removable Media

Beacon:
- Uses secure cloud-based storage where possible
- Backs up important data regularly
- Restricts the use of USB drives and removable media

Unapproved devices must not be used to store Beacon data.

12. Cyber Incidents and Data Breaches

A cyber incident may include:

- Unauthorised access to systems
- Loss or theft of devices
- Phishing or malware attacks
- Accidental data sharing

All incidents must be reported immediately to the Information Security Lead.

13. Cyber Incident Response

In the event of a cyber incident, Beacon will:

- Take immediate steps to contain the issue
- Assess the risk and impact
- Secure systems and change passwords if required
- Inform the Head of Provision
- Notify the ICO or other bodies where legally required
- Communicate with affected parties where appropriate

Incidents are recorded and reviewed to prevent recurrence.

14. Training and Awareness

Staff receive guidance on:

- Cyber security risks
- Safe use of technology
- Data protection responsibilities

Students are supported to use technology safely and appropriately.

15. Monitoring and Review

Cyber security arrangements are monitored through:

- Incident reviews
- System checks
- Staff feedback

This policy is reviewed annually or sooner if required following a cyber incident or change in guidance.

16. Related Policies

- Online Safety and Technology Policy
- Data Protection Policy
- Safeguarding and Child Protection Policy
- Incident Reporting Policy
- Staff Code of Conduct