Beacon Alternative School CIC (and Alternative Provision)

Online Safety and Technology Policy

Date: October 2025
Written by: O'Connell/Field
Review Due by: October 2026

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 sites used by Beacon AP, including home-based teaching at **28 Warwick Road, Exeter, EX1 3HB**, and any other approved venues. It applies to all students, staff, volunteers, and third-party users accessing technology provided or managed by Beacon AP.

1. Introduction

Beacon Alternative Provision recognises the importance of technology in enhancing learning and preparing students for a digital world. This policy sets out the standards, responsibilities, and procedures for safe and responsible use of technology to ensure that all users are protected from harm and data is secure.

2. Purpose

This policy aims to:

- Define acceptable use of technology by students, staff, and other users.
- Outline measures to protect users and data.
- Ensure compliance with **relevant laws and regulations**, including KCSIE 2025, GDPR 2018, and the Data Protection Act 2018.
- Support the safeguarding of students in online environments, including preventing exposure to harmful content or contact.

3. Scope

This policy applies to:

- All students enrolled in Beacon Alternative School and AP programmes.
- All staff, volunteers, and third-party personnel using Beacon Alternative School technology.
- All devices and platforms provided or managed by Beacon, including laptops, tablets, mobile devices, online learning platforms, and communications tools.

4. Acceptable Use of Technology

4.1 General Principles

- **Educational Use:** Technology is provided primarily for educational purposes. Personal use should not interfere with learning.
- **Respectful Communication:** Users must communicate respectfully online. Bullying, harassment, or inappropriate content will not be tolerated.
- **Digital Citizenship:** Users must act responsibly online and understand the impact of their actions on others.

4.2 Student Use

- **Supervised Access:** Students will be monitored to ensure technology is used safely and effectively.

- **Internet Safety:** Students must not share personal information online, access inappropriate content, or engage with unknown contacts. Concerns must be reported to staff immediately.
- **Device Care:** Students are responsible for using devices appropriately and reporting damage or technical issues promptly.

4.3 Staff Use

- **Professional Conduct:** Staff must use technology professionally, respecting student privacy and safeguarding requirements.
- **Data Protection:** Staff must manage student data securely and confidentially, following GDPR and DfE guidance.
- **Monitoring and Support:** Staff are responsible for supervising student use of technology and providing guidance for safe, effective engagement.

5. Cybersecurity Measures

5.1 Network and Device Security

- Firewalls, content filters, and secure password-protected connections protect against unauthorised access.
- Antivirus and security software must be kept up-to-date.
- Devices must receive regular software updates and security patches.
- Lost or stolen devices must be reported immediately to the Head of Provision.

5.2 Data Protection

- Sensitive student data must be encrypted and stored securely.
- Access to personal or confidential information is restricted to authorised personnel.
- Regular backups are maintained to prevent data loss.

5.3 User Training and Awareness

- Staff and students receive regular training on online safety, cybersecurity, and acceptable use of technology.
- Awareness campaigns inform users about emerging online risks and safe practices.

6. Monitoring and Enforcement

- Beacon AP reserves the right to **monitor technology use** to ensure policy compliance.
- Breaches of this policy may result in:
    - Restricted access to devices or online services
    - Disciplinary action in line with staff or student conduct procedures
    - Reporting to external authorities if required by law or safeguarding obligations

7. Safeguarding and Online Protection

- All online activity is subject to the safeguarding policies of Beacon Alternative School and AP.
- Staff must report any concerns about online safety immediately to the **Designated Safeguarding Lead (DSL)**.
- Students must be educated on recognising and reporting harmful online content, including:
    - Cyberbullying
    - Grooming or exploitation
    - Radicalisation or extremist material
    - Inappropriate sexual content

- Links to external guidance:
    - **NSPCC / CEOP:** https://www.ceop.police.uk/safety-centre

8. Remote Learning and Off-Site Use

- When students access technology off-site, staff must ensure supervision, guidance, and risk mitigation measures are in place.
- Home environments used for learning must be assessed for safety, including technology and internet security.

9. Record-Keeping

- Records of **online safety incidents**, breaches, or concerns are maintained in the **Online Safety Log**.
- Health and safety-related incidents involving technology are also recorded in the **Health and Safety Log**.
- Logs are reviewed regularly to identify risks, patterns, and areas for improvement.

10. Review of the Policy

- This policy will be **reviewed annually** or sooner if there are changes in technology, safeguarding guidance, or statutory requirements.
- Amendments will be made in consultation with staff, students, and other stakeholders to maintain compliance and best practice.

11. Roles and Responsibilities

Head of Provision

- Overall responsibility for implementing and reviewing the online safety policy.
- Ensures staff receive appropriate training and support.

Designated Safeguarding Lead (DSL)

- Oversees safeguarding concerns arising from online activity.
- Maintains records of incidents and ensures reporting to relevant authorities.

Staff

- Monitor student technology use and enforce safe practices.
- Report any breaches or concerns promptly.

Students

- Follow the acceptable use policy and report any unsafe or inappropriate online activity.