Beacon Alternative Provision

Use of Technology Policy

1. Introduction

Beacon Alternative Provision recognises the importance of technology in enhancing the educational experience of students. This policy outlines the acceptable use of technology by students and staff, ensuring that all users benefit from a safe and secure digital environment.

2. Purpose

The purpose of this policy is to:

- Define acceptable use of technology by students and staff.
- Outline the cybersecurity measures in place to protect users and data.
- Ensure compliance with relevant laws and regulations.

3. Scope

This policy applies to all students, staff, and any other individuals using technology provided by Beacon Alternative Provision.

4. Acceptable Use of Technology by Students and Staff

4.1 General Principles

- **Educational Use:** Technology provided by Beacon Alternative Provision must be used primarily for educational purposes. Personal use should be limited and must not interfere with educational activities.
- **Respectful Communication:** All users must engage in respectful and appropriate communication online. Bullying, harassment, and inappropriate content will not be tolerated.
- **Digital Citizenship:** Users are expected to act as responsible digital citizens, understanding the impact of their actions online.

4.2 Student Use

- **Supervised Access:** Students will have supervised access to technology to ensure it is used appropriately and effectively for learning.
- **Internet Safety:** Students must follow guidelines for safe internet use, including not sharing personal information and reporting any inappropriate content or contacts to their tutor.
- **Device Care:** Students are responsible for the care and appropriate use of any devices provided to them. Any damage or technical issues should be reported immediately.

4.3 Staff Use

- **Professional Conduct:** Staff must use technology in a manner that upholds professional standards. Personal use should be minimal and not interfere with work responsibilities.
- **Data Protection:** Staff must ensure that all student data is handled in compliance with data protection regulations, keeping information secure and confidential.
- **Monitoring and Support:** Staff are responsible for monitoring student use of technology and providing support to ensure effective and safe use.

5. Cybersecurity Measures

5.1 Network Security

- **Firewalls and Filters:** Firewalls and web filters are in place to protect against unauthorised access and inappropriate content.
- **Secure Connections:** All devices must use secure, password-protected connections to access the internet and Beacon's network.

5.2 Data Protection

- **Encryption:** Sensitive data must be encrypted to protect against unauthorised access.
- **Regular Backups:** Data backups are performed regularly to ensure information is not lost in case of a technical failure.
- **Access Controls:** Access to sensitive information is restricted to authorised personnel only.

5.3 Device Security

- **Antivirus Software:** All devices must have up-to-date antivirus software installed to protect against malware.
- **Software Updates:** Regular software updates must be performed to ensure all security patches are applied.
- **Lost or Stolen Devices:** Any lost or stolen devices must be reported immediately to initiate appropriate security measures.

5.4 User Training and Awareness

- **Training Sessions:** Regular training sessions on cybersecurity and the acceptable use of technology will be provided to all students and staff.
- **Awareness Campaigns:** Ongoing awareness campaigns will be conducted to keep users informed about current cybersecurity threats and safe practices.

6. Monitoring and Enforcement

- **Monitoring Usage:** Beacon Alternative Provision reserves the right to monitor the use of technology to ensure compliance with this policy.
- **Violations:** Any violations of this policy will be addressed promptly. Consequences may include restricted access to technology, disciplinary action, or involvement of law enforcement if necessary.

7. Review of the Policy

This policy will be reviewed annually to ensure it remains effective and up-to-date with current technology and cybersecurity standards. Any necessary amendments will be made in consultation with staff, students, and other stakeholders.

By adhering to this policy, Beacon Alternative Provision aims to provide a safe, respectful, and effective digital environment that supports the educational goals of all students and staff.