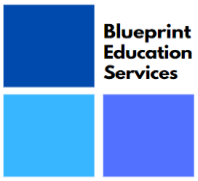
Blueprint Education Services - IT Security Policy
November 2024



1. Purpose

The purpose of this IT Security Policy is to protect the information assets of Blueprint Education Services (BES) from all threats, whether internal or external, deliberate or accidental.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at BES, including all personnel affiliated with third parties. It covers all information assets, including data, systems, and networks.

3. Roles and Responsibilities

- **IT Lead**: Responsible for implementing and maintaining the IT security policy.
- **Employees**: Responsible for adhering to the IT security policy and reporting any security incidents.
- **Third Parties**: Must comply with the IT security policy when accessing BES's information assets.

4. Security Measures

4.1 Access Control

- Access to information systems is granted based on the principle of least privilege.
- Multi-factor authentication (MFA) is required for accessing sensitive systems.
- Audits of access rights are conducted as part as the annual GDPR review.

4.2 Data Protection

- All sensitive data must be encrypted both in transit and at rest.
- Regular backups of critical data are performed and stored securely.

- Data retention policies are in place to ensure data is not kept longer than necessary.

4.3 Incident Response

- An incident response plan is established and regularly updated.
- All employees must report security incidents immediately to the IT Lead.

5. Compliance

- This policy complies with relevant laws and regulations, including GDPR and other applicable data protection laws.
- Compliance audits are conducted to ensure adherence to legal and regulatory requirements.

6. Training and Awareness

- All employees receive regular training on IT security best practices.
- Security awareness programmes are conducted to keep employees informed about the latest threats and safe practices.

7. Monitoring and Review

- Continuous monitoring of IT systems is performed through BES antivirus software to detect and respond to security threats. All file and print systems are within MS365 and so are subject to further checks carried out within Microsoft cloud environment.
- This policy is reviewed annually and updated as necessary to address new threats and changes in the business environment.

8. Enforcement

- Violations of this policy may result in disciplinary action, up to and including termination of employment.