Beacon Academy Trust
A COMPELLING VISION FOR SUCCESS

CYBER SECURITY POLICY

This policy applies to

Beal High School (Centre number 13317)

The Forest Academy (Centre number 13313)

Beacon Business and Innovation Hub (Centre 13362)

Area/Department responsible for policy	TRUST
Approval Body:	Trust Executive
Date of last review:	October 2025
Statutory (DFE) Yes/No	No

1. Introduction

Beacon Multi Academy Trust (BMAT) is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education guidance.

2. Scope

This policy applies to all staff, students, governors, and any third parties who have access to the IT systems and data in any BMAT centre.
This policy will be reviewed annually and updated as required.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre	Overall responsibility for policy implementation and cyber security strategy.
Intersys	Implement technical controls, monitor systems, respond to incidents, manage access and updates.
Data Protection Officer	Ensure compliance with data protection law, advise on data handling, and oversee data breaches.
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Governors	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

BMAT centres implement the following security measures, scaled to our size and needs:

- Firewalls and network security controls.
- Anti-virus and anti-malware software on all devices.
- Regular software updates and patch management.
- Secure data backup and tested recovery procedures.
- Encryption for sensitive and personal data.
- Multi-factor authentication (MFA) for critical systems and remote access.
- Secure configuration and monitoring of cloud services (Office 365).
- Prompt removal of access for leavers.

5. User Account Management

- Password governance must follow NCSC Guidance:
  - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
  - https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
- Access control and permissions are based on job roles and reviewed regularly.
- Accounts are promptly disabled when users leave.
- Account activity is monitored and audited.

6. Staff Training and Awareness

- All staff must complete annual cyber security training and annual refresher training including phishing awareness and social engineering defence training.
- Records of cyber training are retained for all staff and are available for inspection.

7. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to the data protection officer immediately.

Steps for identifying and reporting incidents	All staff must remain vigilant for signs of cyber security incidents, including: • Unauthorised access to exam materials or systems online • Suspected or reported data breaches involving candidate information • Malware/ransomware affecting exam-related systems • Loss or theft of devices containing exam materials • Suspected phishing attempts targeting exam officers • System failures during live assessments Any staff member with concerns must report these directly to the Data Protection Officer (DPO) and Exams Manager. They will gather any appropriate evidence and then decide if the incident needs further investigation or response.
Incident response team	- **Incident Lead** – Data Protection Officer and/or Head of Centre as appropriate. They have overall authority; decision making powers and will be responsible for external communications. Roles within this can be delegated to: o Co-Headteachers/Heads of School o Exams manager o Members of SLT o Members of the Trust Executive can deputise for Incident Lead if unavailable The Data Protection officer will also be responsible for data breach assessment and ICO reporting as appropriate. - **Exams Manager** – First point of contact, incident logging, awarding body liaison Roles within this can be delegated to:

	○ Exams officers - **IT Managed Service Provider – Intersys** - Technical investigation, system isolation, recovery - **SLT** – support, follow up, communication, resource allocation, roles as allocated by Head of Centre.
Communication plan for stakeholders	**Immediate (within 24 hours):** • **Relevant Awarding Organisation(s)**: (AQA/Pearson/OCR/WJEC/etc.) ○ Contact via their incident reporting channels ○ Provide: incident nature, affected qualifications, candidate numbers, containment actions **If data breach involves personal data (within 72 hours):** • Legal advice may be taken. • **Information Commissioner's Office (ICO)**: If appropriate based on ICO guidelines if data breach affects candidate data • **National Cyber Security Centre (NCSC)**: For significant cyber attacks **As appropriate:** • **Parents/Candidates**: If personal data compromised or exam arrangements affected • **Police**: If criminal activity suspected (e.g., theft, hacking) • **Insurance provider (RPA)**: If financial loss or liability
Referral to awarding organisation	The centre will immediately notify the relevant awarding organisation(s) when: • Exam papers or materials are potentially compromised • Candidate data has been accessed unauthorised • Systems used for exam administration are affected • There is any threat to the integrity of the exam process • A cyber incident may impact exam delivery or results
Post-incident review process	A post-incident review will be completed, including as appropriate: - Response effectiveness evaluation - Root Cause Analysis - Documentation for further follow up ○ Additional security measures required ○ Additional training required ○ Improvements to systems required ○ External follow up ○ Any updated cybersecurity procedures required