Policy document control box	
Policy title	**Red Balloon Educational Trust** **Cyber Security Policy** **DRAFT**
Policy owner (including job title)	Maddy Fretwell Head of Data, Systems and Infrastructure, Data Protection Officer
Version	1.00
Red Balloon approving body	Red Balloon Educational Trust (RBET) Trustees
Approving signature	
Approval Date	October 2025
Date of next review	October 2026

Important contacts		
Role	**Name**	**Contact details**
Head of Data, Systems and Infrastructure, Data Protection Officer	Maddy Fretwell	Maddy.fretwell@rbet.ac
IT Provider	Tech Solutions	Techsolutions.co.uk Helpdesk@t7s.co.uk
Head of Centre	Air – Hannah Curry Worthing – Kim Anderson Norfolk – Louise Fisher Aylesbury – Jane Cole	Hannah.curry@rbair.org.uk Kim.anderson@rbet.ac Louise.fisher@rbet.ac Jane.cole@rbet.ac

Policy Contents

1. Introduction 2
2. Scope 2
3. Roles and Responsibilities 3
4. Technical Security Measures 3

Internal Security Measures 3
External Security Measures 4
5. User Account Management 4
6. Staff Training and Awareness 5
Best practice 5
7. Incident Response Plan 5
Procedure for reporting incidents 5
Incident response team 6
Business Continuity and Disaster Recovery 6
Communication plan for stakeholders 6
9. Compliance and Auditing 7
10. Links with other policies 7
11. Policy Review 7
12. Relevant External Organisations 7

1. Introduction

Red Balloon Educational Trust (RBET) is committed to safeguarding its information assets, IT systems, and the personal data of learners, 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. This policy has been developed in alignment with the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education guidance.

Additional guidance includes:

- The Charity Commission guidance: Protect your charity from cyber crime - GOV.UK
- Department for Education guidance: Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK

2. Scope

Red Balloon Educational Trust comprises of Central Services and four Centres: Red Balloon of the Air (RBAir), RBET-Worthing, RBET- Norfolk and RBET- Aylesbury. This policy applies to all staff, learners, trustees, governors, volunteers and any third parties who have access to RBET's IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Head of Data, Systems and Infrastructure	Maddy Fretwell *Overall responsibility for policy implementation and cyber security strategy across the Trust.*
Head of Centre	See important contacts above. *Overall responsibility for policy implementation and cyber security strategy within the relevant Centre.*
IT Provider	Tech Solutions *Implement technical controls, monitor systems, respond to incidents, manage access and updates.*
Data Protection Officer	Maddy Fretwell *Ensure compliance with data protection law, advise on data handling, and oversee data breaches.*
All Staff/ Contractors/ Volunteers	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Governors/Trustees	Oversee and review cyber security arrangements and policy compliance.
Learners	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

Internal Security Measures

Cyber security has been identified as a significant risk for all organisations therefore RBET has invested in a provider and suitable measures alongside staff training to mitigate the risk of falling victim to cyber-crime. The IT Provider, Tech Solutions, is a Managed Service Provider (MSP) that demonstrates a strong commitment to security and quality through its accreditations: Cyber Essentials Plus, ISO 27001, and ISO 9000. The technical security measures required to secure these accreditations and managed by Tech Solutions enable the organisation to function safely.

Cyber Essentials Plus ensures that the organisation has implemented robust technical controls to protect against common cyber threats, including secure configuration, access control, and malware protection. ISO 27001 provides a structured framework for an

Information Security Management System (ISMS), ensuring continuous risk assessment, incident response, and data protection practices. ISO 9000 compliments this by enforcing quality management principles, ensuring consistent service delivery and process improvement.

These certifications collectively support a zero trust and least privilege approach. Cyber Essentials Plus enforces strong perimeter and endpoint security, reducing the attack surface. ISO 27001 mandates strict access controls, encryption, and monitoring, aligning with zero trust principles where no user or device is inherently trusted. Least privilege is embedded through role-based access and regular audits, ensuring users only have the minimum permissions required. Together, these standards create a layered security posture that mitigates risk and ensures compliance with best practices.

RBET implements 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.
- Encryption for sensitive and personal data including third-party softwares.
- Multi-factor authentication (MFA) for critical systems and remote access.
- Secure configuration and monitoring of cloud services (e.g. Office 365).
- Prompt removal of access for leavers.

External Security Measures

RBET is covered by Cyber Insurance which includes broad cyber coverage and cyber-attack prevention services. This service includes constant and pro-active monitoring to identify threats and risks that could impact the organisation such as searching the dark web and hacker forums for compromised organisation credentials and any other malicious activity.

Personal Devices

The above internal and external security measures are applicable to all RBET devices however, where a personal device is in use this must comply with the RBET Bring Your Own Device policy. Use of personal devices to access RBET systems and data is prevented where possible however, the Trust acknowledges there may be individuals who require the use of a personal device.

5. User Account Management

- Password governance should 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 across all systems in use within RBET are based on job roles and responsibilities and reviewed regularly.
- Accounts are promptly disabled when users leave the organisation.
- Account activity is monitored and audited.

6. Staff Training and Awareness

In alignment with the recommendations of Keeping Children Safe in Education (Sept 2025), all staff must complete annual cyber security training to keep up with evolving cyber-crime technologies.

Across RBET all staff are required to read and understand this policy as well as complete The Key's course available here: Cyber security in schools. Records of cyber training is retained for all staff is available for inspection.
This course covers:

- Phishing awareness
- Creating strong passwords
- What to do in the event of a cyber security breach

In specific relation to examinations, in accordance with JCQ guidance, all relevant staff will complete annual and up-to-date cyber security training alongside any relevant awarding body training and will ensure best practice is enforced by all involved with exams including volunteer invigilators.

Signposting to additional resources is available for all RBET staff on the Central Hub including:

- NCSC - Cyber Security for Schools
- Homepage - UK Safer Internet Centre

Best practice

All members of the RBET community are encouraged to follow best practice as outlined in the Staff ICT Acceptable Use policy. Some considerations include:

- Reporting any security breaches, suspicious activities or mistakes which may cause a cyber security breach
- Avoiding clicking links to unknown websites or downloading content from suspicious emails
- Never circumventing any security measures implemented by the Trust e.g. antivirus software, firewalls etc.

7. Incident Response Plan

Procedure for reporting incidents

All staff members must report any suspected security incidents or concerns to the RBET Data Protection Officer (dpo@rbet.ac) and the IT Provider (helpdesk@t7s.co.uk) by email immediately.

If an incident is identified by external security measures the nominated contacts will be informed directly. The nominated contacts for RBET are:

- Leanne Thurston – Director of Finance and Operations
- Maddy Fretwell – Head of Data, Systems and Infrastructure, Data Protection Officer

Incident response team

The RBET Data Protection Officer and the IT provider (TechSolutions) will handle the initial response to any cyber security incidents. This will include notifying the Cyber Insurance provider whose team of experts will provide support and guidance to triage, contain and recover any data. Once reviewed, any other relevant persons will be contacted and roles/actions identified which may include the Head(s) of Centre, Administrators, members of the Senior Leadership Team and Exams Officers.

Where a cyber security incident involves a personal data breach the Trust will invoke the Data Breach Policy which will run alongside a cyber incident response process or instead of dependent upon the identified situation.

Once an incident has been reviewed and contained, a post-incident review process will be carried out to identify lessons learned, upskill staff where required and update any relevant procedures if necessary.

Business Continuity and Disaster Recovery

Maintaining functionality and business continuity is of the utmost importance for RBET to prevent any negative impacts for the community and the organisation. As a 'Cloud-native' organisation, devices are considered secure because they are built on zero-trust principles and leverage strong identity-based access controls, such as multi-factor authentication and conditional access policies. They use hardware-based security like TPM chips and secure boot to ensure system integrity, while compliance policies, encryption, and remote wipe capabilities are enforced continuously through the cloud. Additionally, these devices avoid legacy protocols that ransomware often exploits and receive automatic updates adhering to Cyber Essentials guidelines that limit attack surfaces.

CryptoLocker and similar ransomware rely on lateral movement through flat networks. When geographic sites are segmented by firewalls, east-west traffic is restricted, preventing unauthorised communication between sites. This segmentation means that even if one site is compromised, the malware cannot propagate to others because the firewall enforces strict rules and isolates network zones. Combined with zero-trust and least-privilege principles, this approach significantly limits the potential data at risk.

In addition to the support provided by, and structure maintained by the IT provider, the Cyber Insurance provider will engage with the organisation to contain and remediate the incident. Once contained, their incident response team will work to rebuild systems and reconstitute data.

Communication plan for stakeholders

Where a cyber security incident has been identified and reported, communication will be led by the Data Protection Officer and IT Team in collaboration with the Director of Finance and Operations, and Head(s) of Centre. This may include but is not limited to informing staff, learners, parents/carers or other members of the RBET community, relevant exam awarding bodies, the National Cyber Security Centre (NCSC), the Information Commissioner's Office, The Charity Commission, OFSTED and the relevant Local Authorities.

9. Compliance and Auditing

- Automatic auditing: Requiring Intune enrolment provides an automatic compliance audit mechanism. Devices that fail to install updates within the defined timeframe or fall out of compliance are automatically flagged and are blocked from accessing any company resources. This continuous monitoring and enforcement reduce reliance on manual checks and ensures that non-compliant devices are quickly identified and remediated. Together, timely patching and automated compliance auditing create a proactive security framework that limits risk and maintains a strong defence against evolving threats.

10. Links with other policies

This policy should be read in conjunction with:

- RBET Safeguarding and Child Protection Policy
- RBET Online Safety Policy
- RBET Data Protection Policy
- RBET Staff ICT Acceptable Use Policy
- RBET Bring Your Own Device Policy

11. Policy Review

This policy will be reviewed annually by the policy owner with collaboration from the IT Provider. This policy will be updated as necessary to reflect changes in technology, threats, and best practices.

12. Relevant External Organisations

OFSTED	Ofsted - GOV.UK
Information Commissioners Office	https://ico/org.uk
National Cyber Security Centre (NCSC)	National Cyber Security Centre - NCSC.GOV.UK
JCQ – Joint Council for Qualifications	Contact - JCQ Joint Council for Qualifications
National Crime Agency	Home - National Crime Agency