Policy document control box	
Policy title	**Red Balloon Educational Trust** **Bring Your Own Device 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	
Date of next review	

Important contacts		
Role	Name	Contact details
RBET Head of Data Systems and Infrastructure, Data Protection Officer	Maddy Fretwell	Maddy.fretwell@rbet.ac
IT Provider	Tech Solutions	Helpdesk@t7s.co.uk

Policy Contents

1. Purpose

Red Balloon Educational Trust (RBET) comprises Central Services and four Centres: Red Balloon of the Air (RBAir), RBET-Worthing, RBET-Norfolk and RBET-Aylesbury. This Bring Your Own Device (BYOD) policy outlines the requirements and responsibilities for employees, governors, trustees, volunteers, contractors, sub-contractors, learners and all other members of the RBET community who use personal devices to access organisational data or services, in compliance with Cyber Essentials.

RBET aims to:

- have robust processes in place to ensure compliance with UK GDPR legislation;
- identify and support all members of the RBET community to fulfil their roles whilst protecting both RBET data and the privacy of the user's personal data

2. Scope

This policy applies to all user-owned devices that access RBET organisational data or services, except those used solely for:

- Multi-Factor Authentication
- Native text applications
- Native voice applications

3. Legislation and guidance

This policy is based on the UK Data Protection legislation and national guidance including:

- Cyber Essentials - NCSC.GOV.UK
- ICO Bring Your Own Device Guidance

4. Responsibilities

The RBET Data Protection Officer (DPO) and External IT Provider

The RBET DPO and external IT provider are responsible for:

- putting in place an appropriate level of security protection, to prevent access to internal systems on unapproved personal devices including conditional access restrictions;
- maintaining full security and monitoring of RBET ICT systems, as per contractual obligations;
- ensuring RBET remain compliant with Cyber Essentials accreditation, applying annually for certification renewal.

This list is not intended to be exhaustive.

All Staff, Trustees, Governors, Contractors and Volunteers

All users of personal devices to access RBET data or services must:

- not use personal devices where access to an RBET device is available;
- understand, implement and adhere to this policy, the RBET Cyber Security Policy and the RBET Staff ICT Acceptable Use Policy;
- ensure their devices meet the security requirements outlined in this policy;
- not to attempt to circumvent any RBET restrictions including conditional access, network security and/or filtering systems;
- Report any security incidents or lost/stolen devices immediately to the RBET DPO via email: dpo@rbet.ac and the relevant Head of Centre to ensure mitigations are put in place.

5. Device Management

Any personal device used for work purposes accessing RBET resources must comply with the following, access will only be granted if agreed by the RBET DPO. Any device that does not comply or poses a security risk will be denied access until it is made compliant, and evidenced, to meet the below criteria:

- Minimum standards of hardware and software versions must be met and supported by the manufacturer.
- Be protected by a strong, unique password or passphrase.
- Running latest supported operating system.
- Have the latest security and critical updates applied on the device.
- Where available running a firewall.
- Where available running an antivirus application.
- Not have any inappropriate software running such as Crypto miners, malware etc. which pose significant cyber security risk to the RBET network.
- If used in a Centre, not display any inappropriate/offensive messages/visuals.

All BYOD devices must implement strong access policies and security controls. While traditional centralised administration ensures consistency, BYOD introduces variability. Therefore, access to organisational data and services must be enforced through robust policies.

When applying for the use of a personal device, all individuals will be asked to complete a BYOD questionnaire. Completion of this questionnaire requires individuals to acknowledge their responsibility to maintain appropriate security practices with the understanding that should a cybersecurity incident occur due to a lapse in these measures, they may be held accountable.

AI regulation

Due to the rapidly evolving nature of AI software's, if an AI tool is downloaded or in use on a personal device, the user must disclose this to the RBET DPO at the time of applying for use of a personal device or at any point post permission if the situation changes.

6. Home Working and Purpose of BYOD

All RBET or BYOD devices used for business purposes at home are in scope for Cyber Essentials. ISP routers and user-provided routers are out of scope. Devices must implement software firewalls unless a company-provided router is used. If an RBET VPN is used, the internet boundary is defined by the company firewall or virtual/cloud firewall.

Personal devices should only be used for work purposes when required, if access to an RBET device is available to the individual then work and access should be completed on the RBET device.

Unpermitted use:

- Users should not download RBET resources onto their personal device unless there is valid reason to do so, if downloaded all RBET resources should be deleted from the device as soon as possible to prevent the risk of future data breaches.

7. User Access Control

To comply with Cyber Essentials v3.0:

- All devices must have separate user and administrator accounts.
- Users must operate under standard user accounts for daily activities.
- Administrator accounts must only be used when elevated privileges are required.
- This separation reduces the risk of malware and unauthorised changes to system configurations.

8. Enforcement

Failure to comply with this policy may result in disciplinary action and revocation of BYOD privileges. RBET will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Review

This policy will be reviewed annually or upon significant changes to Cyber Essentials or UK GDPR requirements.

10. Training

All new staff members, trustees, governors and volunteers will receive training, as part of their induction, on safe internet use and online safety. These principals should be applied when using both RBET and personal devices to ensure the protection of RBET data and individual privacy.

More information about safeguarding training and data protection is set out in our Safeguarding and Child Protection Policy and Data Protection Policy and privacy notices.

11. Links with other policies

This Bring Your Own Device Policy should be read in conjunction with our other relevant policies including:

- RBET Data Protection Policy and Privacy Notices
- RBET Staff ICT Acceptable Use Policy
- RBET Cyber Security Policy
- Staff Code of Conduct