RedBalloon
Educational Trust

Policy document control box	
Policy title	**Red Balloon Educational Trust Staff ICT Acceptable Use Policy**
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	Carrie Herbert
Approval Date	August 2025
Date of next review	August 2026

Important contacts		
Role	Name	Contact details
Designated Safeguarding Lead (DSL)	Air - Hannah Curry Worthing - Kim Anderson Norfolk - Ellie Rix Aylesbury - Claire Cockcroft	Hannah.curry@rbair.org.uk Kim.anderson@rbet.ac Ellie.rix@rbet.ac Claire.cockcroft@rbet.ac
RBET Head of Data Systems and Infrastructure, DPO (Data Protection Officer), Safeguarding Lead	Maddy Fretwell	Maddy.fretwell@rbet.ac Tel: 01223 354338
IT Service Provider	Tech Solutions	helpdesk@t7s.co.uk 01903 372002
Trustees	RBET Trustees	trustees@rbet.ac

Policy Contents

1. Overview

This policy outlines the acceptable use of information technology resources at Red Balloon Educational Trust (RBET). It aims to protect the integrity, security, and availability of IT resources and ensure their appropriate use in an educational and pastoral environment. IT is a significant learning and communication resource that RBET relies on heavily. Keeping our learners and staff safe is RBET's priority; therefore, there are strict rules in place when it comes to usage.

RBET currently works with an externally contracted IT service provider to configure, monitor and manage all RBET devices.

2. Scope

This policy applies to all teaching and non-teaching staff, contractors, consultants, temporary staff, and other workers at RBET, including all personnel affiliated with third parties. You are responsible for any activity which occurs within your accounts.

RBET applies to: Central Services, Red Balloon of the Air (RBAir), Red Balloon Worthing, Red Balloon Norfolk and Red Balloon Aylesbury.

3. Acceptable Use

General Use: IT resources should only be used for educational and administrative purposes in alignment with business roles and responsibilities.
Security: Users must take reasonable precautions to protect IT resources, including using strong passwords, locking devices when not in use, and reporting any security incidents immediately.
Software and Hardware: Only authorised software and hardware should be used. Installation of unauthorised software or hardware is prohibited.
Email and Communication: School email and communication tools should only be used for professional communication.

4. Prohibited Activities

Unauthorised Access: Accessing IT resources without proper authorisation is strictly prohibited. Under no circumstances should you divulge your password to anyone else nor should you gain access or attempt to gain access to information stored electronically which is beyond the scope of your authorised access level.
Email and Communication: School email and communication tools should not be used for any personal use. You should never log into any work accounts from personal devices, including email and Teams, unless otherwise agreed with the DPO and Headteacher.
Malicious Activities: Engaging in activities that could harm IT resources, such as spreading malware or hacking, is forbidden. You must not tamper with any monitoring, tracking facility or device configurations. Tampering with tracking or monitoring software or devices may lead to action under the Disciplinary Procedure up to and including summary dismissal. This makes up part of your contractual terms

and conditions.

Inappropriate Content: Using IT resources to access, store, or distribute inappropriate or illegal content is prohibited. This includes content that is not suitable for a school environment.

Privacy Violations: Users must respect the privacy of students, staff, and others, and not access or disclose personal information without authorisation. The use of any device to photograph or film fellow employees, visitors, or any member of the public without their consent may breach an individual's right to privacy and could in certain circumstances constitute harassment.

Storage: Individuals should not store personal files, images, software or Apps on the RBET network or devices. Equally, they should not store RBET data on any personal devices.

5. Personal Devices

Unless a personal mobile phone has been approved for work use, you should avoid using your mobile phone during working hours, excluding breaks. Under normal circumstances personal phones should be kept away though we understand that you may have caring or other responsibilities that require you to be contacted during working hours and therefore keeping your phone in close proximity is required.

Unauthorised use of a personal mobile phone during working hours may result in a disciplinary warning or dismissal, depending on the circumstances.

There will be certain exceptions to this, such as:

- You may be required to use your personal mobile number to allow you to manage two-factor authentication if you do not have a work issued mobile;
- The use of personal devices for HR purposes or pre-agreed Red Balloon Educational Trust (RBET) apps and software such as Multi-Factor Authentication or the Sign-In App.

Monitoring of Personal Communications

As stated above, RBET may monitor, intercept or record all communications received or made via RBET's telephone system or any other system including email and internet usage. If unmonitored communication is required for any reason, you should discuss this with your line manager. Monitoring may be conducted by any member of management but will be for work-related purposes only. This makes up part of your contractual terms and conditions.

Social Media and Personal Publishing

Staff and other members of the RBET community are reminded of the risks of accepting parents/carers and learners as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' people from viewing their private pages when appropriate. Staff will be shown how to 'block' their profile picture from being downloaded and protect their profile information. Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites. Teachers are instructed not to run social network spaces for learner use on a personal basis or to open up their own spaces to their learners, but to use the Trust's preferred system for such communications.

RBET staff, contractors and visitors will ensure that in private use:

- No reference should be made in social media to learners, parents / carers or any other members of the RBET community including staff
- They do not engage in online discussion on personal matters relating to members of the Trust community
- Personal opinions should not be attributed to the Trust/Centre
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

6. Relevant Policies

This Policy is associated with RBET's DataProtection Policy, RBET Online Safety Policy and each Centre's Lone Worker Policy, the provisions of which should be adhered to at all times.

RBET will provide annual training for all staff regarding Online Safety, GDPR and other relevant areas of development aligning with this policy. This will be managed by relevant staff at Trust level or individually at each Centre including the Headteacher, Designated Safeguarding Lead, Online Safety Lead and Data Protection Officer.

7. Monitoring and Privacy

Digital monitoring is implemented at RBET to ensure appropriate safeguarding measures for both staff and learners. Smoothwall Monitor and Filter are installed on all RBET devices and are regularly reviewed to ensure efficacy. Please see the RBET Online Safety policy for further details about this software.

8. Enforcement and Acknowledgement

Violations of this policy may result in disciplinary action, up to and including termination of employment. Legal action may also be taken if necessary.

All RBET staff, contractors, volunteers or other users of RBET technology must acknowledge that they have read, understood, and agree to comply with this policy.

The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to RBET Trustees.

If you have any questions or concerns about this policy please contact the policy owner, or those listed as important contacts.