Policy document control box	
Policy title	**Information Security Policy**
Policy owner	Brooke Hornby RBET HR and Operations Lead Maddy Smart RBAir GDPR Lead
Version	1.00
Approving body	
Date of meeting when version approved	November 2023
Date of next review	November 2024

Policy contents:

Contents

1. Overview 3
2. Purpose 3
3. Scope 3
4. Policy 4
5. Roles and Responsibilities 4
6. Acceptable Use Policy 5
   - 6.1 Access Control and Security 5
   - 6.2 Use of Strong Passwords 5
   - 6.3 Mobile Storage Devices 6
   - 6.4 Software and Applications 7
   - 6.5 Software Audits 7
   - 6.6 Anti-Virus and Malware 7
7. Internet and Email Policy 7
   - 7.1 Social Media and Instant Messaging 9
   - 7.2 Remote Access 9

7.3 Actions Upon Employee Leaving the Company 10
7.4 Monitoring and Filtering 10
8. Network Guidelines and Responsibilities 11
8.1 Securing Your Home Network 11
8.2 Workstation and Laptop Security 12
9. Clean Desk Policy 12
10. Vendor Management 13
11. Physical Security and Environmental Security 13
12. Encryption 13
13. Business Continuity/Disaster Recovery Policy 14
14. Security Awareness and Training Policy 14
15. Information Retention and Destruction Policy 15

Information Security

1. Overview

Red Balloon Educational Trust (Red Balloon hereon in) takes the safeguarding and handling of data very seriously. This document (and supporting policies) governs the processing of personal data and defines the technical and security measures that must be implemented to meet the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and ensure integrity and availability of the data environment and services.

2. Purpose

The purpose of this policy is to protect Red Balloon, its stakeholders and staff from all information security threats, whether internal or external, deliberate, or accidental. Red Balloon is critically dependent on information and information systems. If information were disclosed to inappropriate persons, the company could suffer serious reputational damage, where safeguarding our staff and learners is paramount. The good reputation that Red Balloon enjoys is also directly linked with the way that it manages both information and information systems.

Information security is characterised as the preservation of:

- **Confidentiality** - ensuring that information is accessible only to those authorised to have access.
- **Integrity**- safeguarding the accuracy and completeness of information and processing methods.
- **Availability**- ensuring that authorised users have access to information and associated assets when required.

3. Scope

Every member of staff at Red Balloon must comply with the information security policies found in this policy and any related information security documents.

All staff, contractors and third-party users should be made aware of this policy, their responsibilities and liabilities, and any information security threats or concerns.

All information owned or otherwise processed by Red Balloon, at all stages of the information lifecycle: creation, use, storage, disposal, is in scope of this policy.

This policy and supporting procedures encompass all Red Balloon system components, including those that are owned, operated, maintained, and controlled by Red Balloon Educational Trust and all other system components, both internally and externally, that interact with these systems, and all other relevant systems.

Internal system components are those owned, operated, maintained, and controlled by Red Balloon and include all network devices (firewalls, routers, switches, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system components deemed in scope.

External system components are those owned, operated, maintained, and controlled by any entity other than Red Balloon, but for which these very resources may impact the confidentiality, integrity, and availability and overall security of its information and any other environments deemed applicable.

4. Policy

Red Balloon is to ensure that the information security policy adheres to the following conditions for purposes of complying with the mandated organisational security requirements set forth and approved by management:

5. Roles and Responsibilities

All individuals who use Red Balloon information or information systems have a duty of care to protect the confidentially of information that is entrusted to them. The principal information security responsibilities for all are to:

- Only use information and systems that you have authorisation to use
- Follow all relevant instruction, procedures, guidelines, and codes of practice
- Report any real or suspected breaches of information security to your line manager
- Not use, or attempt to use, any information or information system for illegal of inappropriate purposes

The following roles and responsibilities are to be developed and subsequently assigned to authorised personnel within Red Balloon regarding information security practices:

End Users: Responsibilities include adhering to the organisation's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such Red Balloon system components.

Additionally, end users are to report instances of non-compliance to line management, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of Red Balloon system components and are to also report such instance immediately to their line management as required.

Vendors, Contractors, Other Third-Party Entities: Responsibilities for such individuals and organisation are much like those stated for end users: adhering to Red Balloon's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.

HR: Disciplinary matters resulting from violations of information security requirements are handled by local managers working in conjunction with the Human Resources department.

Internal Audit: Compliance checking to ensure that organisational units are operating in a manner consistent with this and related policies.

6. Acceptable Use Policy

This Acceptable Use Policy covers the information security and use of all Red Balloon's IT equipment. It also includes the use of email, internet, and mobile IT equipment. This policy applies to all employees and contractors (hereafter referred to as 'individuals'). This policy applies to all information, in whatever form, relating to Red Balloon business activities and to all information handled by employees relating to other organisations with whom it deals.

6.1 Access Control and Security

Access to information in the possession of, or under the control of Red Balloon must be provided based on the need to know. Information must be disclosed only to people who have a legitimate business need for the information. To implement the need-to-know concept, Red Balloon has adopted an access request and owner approval and review process.

When an employee's role changes, including termination, transfer, promotion and leave of absence, the IT department must be notified.

Access to all IT systems is controlled by user logins, passwords and/or two-factor authentication tools. All logins and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on all Red Balloon's IT systems.

6.2 Use of Strong Passwords

While most passwords will be enforced by group policy settings, it is still important to make them unique, never using information pertaining to your favourites sports team, home address, middle name, etc.

Users can use passwords that are difficult for unauthorised parties to guess if they:

- String several words together.
- Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word.
- Combine punctuation or numbers with a regular word.
- Create acronyms from words in a song, poem, or another known sequence.
- Deliberately misspell a word.
- Combine several preferences like hours of sleep desired and favourite colours.

In line with the most recent guidance issued by the Information Commissioner's Office (ICO), the emphasis should be on making passwords or passphrases difficult or complex to begin with rather than require frequent, enforced changes. Therefore, the password or passphrase should be at least 10 characters long, include upper and lowercase letters and special characters, committed to memory and not written down. The password or passphrase is only to be changed when there is a data breach or whenever a worker suspects that a password/passphrase has become known to another person.

Individuals must not:

- Allow anyone else to use their user login and password on any IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's login and password to access any IT system.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Red Balloon's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Connect any non-authorised device to the Red Balloon network or IT systems (for example personal laptop or computer).
- Store company data on any non-authorised equipment.

6.3 Mobile Storage Devices

To ensure UK GDPR compliance, mobile devices such as USB memory sticks, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. With the implementation of the Microsoft suite, including SharePoint, the need for these devices to be used will be minimal.

Mobile storage devices are never to contain highly sensitive and confidential information, such as Personally Identifiable Information (PII), or any other data deemed privileged. Such information should be transferred over the network using approved protocols and residing on company servers only.

6.4 Software and Applications

Employees must use only software that is authorised by Red Balloon on laptops/computers. Authorised software must be used in accordance with the software licensing agreements. All software on laptops/computers must be approved by the company.

6.5 Software Audits

The company will conduct random software compliance audits on workstations, including laptops, on a regular basis. The audits are for ensuring compliance with software licensing rules, while also ensuring your computers are free of any potentially dangerous applications. These audits are conducted automatically whilst machines are in general operation.

Individuals must not:

- Store personal files such as music, video, photographs, or games on company IT equipment.
- Install unauthorised and/or pirated software that can potentially reduce performance of IT equipment and pose a security risk to company data and network.
- All workers should refrain from taking screenshots that include personal data and saving a copy to their desktop or mobile device.

6.6 Anti-Virus and Malware

The company has implemented centralised, automated virus detection and virus software updates. All computers have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection. Should an infection be suspected, it should be reported to IT immediately, who will resolve the matter.

7. Internet and Email Policy

Use of Red Balloon internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the company in any way, not in breach of any term and condition

of employment and does not place the individual or company in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Internet access is monitored to ensure that workers continue to be in compliance with security policies.

All information received from the Internet should be considered to be suspect until confirmed by reliable sources.

Every Red Balloon member of staff who uses computers in the course of their regular job duties will be granted an Internet electronic mail address and related privileges. All business communications sent by electronic mail must be sent and received using this company electronic mail address.

When transmitting messages to groups of people outside Red Balloon, workers must always use either the blind carbon copy facility or the distribution list facility. Note that unsolicited electronic mail transmissions to prospects and customers are prohibited.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Red Balloon considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the internet that relates to the company, alter any information about it, or express any opinion about the company, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally
- Forward company mail to personal email account.
- Download copyrighted/licensed material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Download any software from the internet without prior approval of the company.

7.1 Social Media and Instant Messaging

Red Balloon recognises that there is legitimate business, and personal, reasons for using social media at work or using company computing resources. To enable employees to take advantage of the business value of these sites and to promote an open, trusting, collaborative workplace, Red Balloon allows company employees to use social media within the guidelines specified below.

Social media includes any website in which visitors can publish content to a larger group. Content shared may include (but is not limited to) personal information, opinions, research, commentary, video, pictures, or business information. Examples of such destinations include large, branded entities such as Facebook, Twitter,

YouTube, and LinkedIn. However, blogs, special interest forums, user communities are also considered social media.

You must use caution when using social networking for communication. You must use social networking sites in a professional and responsible manner.

- It is your responsibility to ensure the social media account is protected by enabling the privacy settings available.
- Inappropriate content should not be accessed by employees while at work, or while using company resources, employees should use common sense and consideration for others in deciding which content is appropriate for the workplace.
- It is the responsibility of the employee to ensure that personal business does not affect work quality or productivity.
- **DO NOT** use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the workplace.

7.2 Remote Access

All access to Red Balloon systems initiated outside the organisation’s trusted network infrastructure is to be considered "remote access". All users are to utilise approved technologies, such as secure private networks, to connect to Red Balloon systems.

The concept of two-factor authentication, along with strong password policies creates yet another layer of security relating to access rights for all authorised users granted remote access into Red Balloon’s network.

The following controls must be applied:

- IT equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Information should be protected against loss or compromise when working off-site or in public places.
- All RBET laptops are encrypted by default, with the keys stored in Azure
- Extra care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. By default, all RBET devices will be set up with a minimum of a password or a PIN and encryption.

7.3 Actions Upon Employee Leaving the Company

All company equipment and data, for example laptops and mobile devices including telephones and USB memory devices must be returned to Red Balloon upon leaving the company. Users will not be allowed to have any e-mails forwarded to them once they have left.

All company data or intellectual property developed or gained during the period of employment remains the property of Red Balloon and must not be retained beyond departure or reused for any other purpose.

7.4 Monitoring and Filtering

All data that is created and stored on company computers is the property of Red Balloon and there is no official provision for individual data privacy, however wherever possible Red Balloon will avoid opening personal emails.

IT systems activity is continuously logged, and investigations will be commenced where reasonable suspicion of a breach of security or policy exists. Red Balloon has the right to monitor activity on its systems, including internet and email use, to ensure systems security, effective system operation and to protect against misuse. Any monitoring will be carried out in accordance with controlled internal processes and in compliance with the follow acts:

- the Data Protection Act 2018
- the Regulation of Investigatory Powers Act 2000
- the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000
- UK GDPR
- Computer Misuse Act 1990

It is your responsibility to report suspected breaches of security policy without delay to your line management or the IT support partner.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Red Balloon disciplinary procedures.

8. Network Guidelines and Responsibilities

Red Balloon has established the following general guidelines, responsibilities, and acceptable uses for network devices as described below.

- All network devices are to be configured and used strictly for business operations (outside of what is permitted by the Internet and Email Policy above).
- All users must be responsible for the proper use of these devices.
- All activities undertaken on network devices are subject to audit and review as needed.

The following activities are considered unacceptable by users.

- Modifying network devices regarding system settings without documented approval and business justification is strictly prohibited.
- Network components may not be added, removed, or modified unless explicit consent is given by IT.
- Utilising another employees log in credentials, unless prior authorisation from either IT or senior management has been granted.

8.1 Securing Your Home Network

Where employees work from home, which means they store, process, and transmit sensitive and confidential information over their personal networks, this can pose significant security risks.

Please follow the best practices for securing your home/personal network equipment:

- Only approved company equipment should be used to access company systems.
- Use strong passwords. Whatever you are doing online, it's a good idea to use very strong password, those that contain a mixture of letters, numbers, and symbols. This applies to your actual computer for which you're logging onto.

- Be cautious online. Remember that working from home means you're accessing Red Balloon information, so be smart about what websites you're visiting, information you are downloading, etc. Being cautious and having a "security first" mindset is always a must.

8.2 Workstation and Laptop Security

Protecting your workstation area is an important duty all employees should take very seriously.

The following best practices should be adhered to:

- Don't alter security settings. Your workstation has been configured for maximum security along with performance, so do not attempt to disable or modify configuration settings to the operating system or any other applications. Doing so may increase security vulnerabilities that would ultimately allow malicious files and other harmful scripts to reside on the workstation.
- Report security issues immediately. Remember, if you see something, report it immediately. You have a responsibility for helping protect the organisation, which means being aware of your surroundings and reporting suspicious activity to authorised personnel immediately.
- Shut down and protect your workstation. When leaving your workstation area at the end of each day, make sure to completely shut down and turn off all computers and related devices. Additionally, pickup and store any documents that should not be left unattended. Use your judgment by asking yourself the following simple question – “what risk or security danger is there for leaving something not securely locked up and put away?”
- If your laptop is stolen, think and act quickly. Report the theft to the police along with informing management and IT immediately.

9. Clean Desk Policy

Keeping your desk free of clutter and unnecessary items helps in promoting a professional work environment, while also ensuring the safety and security of sensitive documents and assets.

Because employees all leave their workstations throughout the day for any number of reasons, make sure to turn off your computers or at the very minimum, enable the password protected screensaver.

For any documents no longer needed, ensure they are shredded or placed in a secure disposal.

10. Vendor Management

Third parties may be given access to internal information only when a demonstrable need to know exists, when a non-disclosure agreement has been signed, and when such a disclosure has been expressly authorised by the relevant information owner.

When using the services of various third-party outsourcing entities, a certain element of risk arises as responsibilities for critical data is in the hands of another organisation.

It's important to understand these risks, what they are, and how Red Balloon can readily identify any issues, concerns, or constraints pertaining to these risks.

Failure to mitigate and prevent these risks can result in significant financial loss, legal issues, and public opinion misconceptions, ultimately damaging the organisation.

11. Physical Security and Environmental Security

Appropriate security measures are to be implemented, which includes all necessary physical security controls, such as those related to the safety and security of Red Balloon systems.

This requires that the use of a computer room or other designated area (facility) is always secured and monitored.

In line with the clear desk policy above, when left in an unattended room, sensitive information in paper form must be secured appropriately. Unless information is in active use by authorised people, desks must be clear and clean during non-working hours to prevent unauthorised access to information.

Workers must position their computer screens such that unauthorised people cannot look over their shoulder and see the sensitive information displayed.

Only authorised personnel will have physical access to the specified systems.

12. Encryption

When necessary and applicable, appropriate encryption measures are to be invoked for ensuring the confidentiality, integrity, and availability of Red Balloon systems and any sensitive data associated with them. Additionally, any passwords used for accessing and/or authentication to the specified systems are always to be encrypted, as passwords transmitting via clear text are vulnerable to external threats. As such, approved encryption technologies, such Transport Layer Security (TLS) and other

secure data encryption protocols are to be utilised when accessing the specified system component.

Additional encryption measures for Red Balloon are to also include the following best practices for all applicable devices that have the ability to store sensitive and confidential information:

Servers - Depending on the type of server and the underlying applications, a large range of encryption measures can be adopted. The first measure is identifying the type of information residing on such servers and the necessary encryption protocols to apply. Additionally, servers are to be provisioned and hardened accordingly, with anti-virus also installed.

Non-company owned devices, such as those physically located at an employee's home, are to never contain organisational information under any circumstances. If such data needs to be accessed for performing remote duties, then a secure connection must be made to the Red Balloon network for accessing all relevant information. Additionally, laptops, mobile computing devices, and smart devices are to be provisioned and hardened accordingly, with anti-virus also installed.

Email encryption is encryption of email messages to protect the content from being read by other entities than the intended recipients. Email encryption may also include authentication.

In our Microsoft Infrastructure, messages are encrypted at rest and while in transit between data centres. Messages transiting to third-party providers are encrypted with Transport Layer Security when possible.

13. Business Continuity/Disaster Recovery Policy

Documented Business Continuity and Disaster Recovery Planning (BCDRP) are vital to protecting all Red Balloon assets along with ensuring rapid resumption of critical services in a timely manner.

Because disasters and business interruptions are extremely difficult to predict, it is the responsibility of authorised Red Balloon personnel to have in place a fully functioning BCDRP process, and one that also includes specific policies, procedures, and supporting initiatives relating to all system resources.

14. Security Awareness and Training Policy

All employees within Red Balloon are to undergo annual security and data protection awareness training initiatives for ensuring they stay abreast of significant security

issues that pose a credible threat to the organisation, including, but not limited to, Red Balloon's network infrastructure and all supporting system resources.

While the goal of the programme is to have in place a comprehensive framework that effectively addresses the core components of awareness, training and education, the programme must also provide subject matter directly related to the safety and security of specific system components. Specifically, all users (both end-users and administrators) having access rights to various Red Balloon IT resources must have adequate knowledge in understanding the threats associated to these specified system components, along with the necessary response and resolution measures to undertake.

15. Information Retention and Destruction Policy

It is company policy to limit data storage amount and retention time to that which is required for legal, regulatory, and business requirements. For more information, please see our Data Retention Policy.

Processes are to be in place for secure disposal of data when no longer needed for legal, regulatory, and business requirements. This in turn mandates retention requirements be in place and documented accordingly for all legal, regulatory, and business requirements.

Additionally, a manually executed process is to be in place for identifying and securely removing data that exceeds the defined legal, regulatory, and business requirements. As for disposing of data, the following methods are to be utilised for both hard copy and electronic data:

- Purging and deleting data from all system components. This can be done by utilising a secure wipe program in accordance with industry-accepted standards for secure deletion
- Destroying (cross-shredding) any data that is in a hardcopy format.